ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

Previa obtención del título de:

LICENCIADO EN REDES Y SISTEMAS OPERATIVOS

TESINA DE SEMINARIO:

“IMPLEMENTACIÓN DE UN CONTROLADOR DE DOMINIO SOBRE LINUX”

Autores:

JACKSON ENRIQUE CORTEZ DIAZ

WILSON DANIEL VILLAVICENCIO RIERA

GUAYAQUIL-ECUADOR

2014

AGRADECIMIENTO

A la universidad por ser el escenario perfecto para nuestra preparación, al Ing. Barboza por su enseñanza y guía en este proyecto, a nuestra familia por ser el apoyo fundamental para culminar la carrera.

Los Autores

DEDICATORIA

A mi Dios por estar siempre presente en mi corazón, a mi tía, mis padres y mis hermanos que siempre me han apoyado para logran cumplir con éxito este proyecto de estudio.

DANIEL

A mis padres y hermano que siempre me han apoyado para lograr cumplir con éxito mi carrera.

JACKSON

TRIBUNAL DE SUSTENTACIÓN

Ing. Fabián Barboza

Ing. Albert Espinal

DECLARACIÓN EXPRESA

"La responsabilidad del contenido de esta Tesina, me corresponde exclusivamente; y el patrimonio intelectual de la misma a la Escuela Superior Politécnica del Litoral".

Jackson Cortez

Daniel Villavicencio

RESUMEN

Esta tesis comprende el análisis de dos plataformas, un sistema operativo licenciado como es Windows; otro de código abierto como es CentOS distribución de Linux, y la implementación de una herramienta de código abierto para la interoperabilidad de las plataforma y de esta manera permitir la compartición de sus recursos.

Se han configurado protocolos y empleado paquetes de código abierto en centos para de esta forma permitir que los usuarios del active directory de Windows puedan acceder al centos y a todos los recursos compartidos dentro de este y exista una interoperabilidad entre plataformas.

Se ha desarrollado una herramienta web que facilita a los administradores de servidores y personal de TI en general hacer todo el trabajo de integración entre las plataformas, solo con ingresar los datos necesarios para esta, todo el proceso de integración se realiza de una manera transparente para el operador de la herramienta, la cual maneja funciones y procesos para la comprobación y configuración de los paquetes y protocolos necesarios para permitir una interoperabilidad entre las plataformas, lo cual es un punto clave para un sistema heterogéneo.

ÍNDICE GENERAL

ABREVIATURAS

1. ADS : Active Directory Service
2. AP : Access Point
3. CIFS : Common Internet File System
4. CSS : Cascading Style Sheets
5. DC : Domain Controller
6. DMZ : Demilitarized Zone
7. DNS : Domain Name System
8. DVD : Digital Versatile Disc
9. ERP : Enterprise Resource Planning
10. FQDN : Fully Qualified Domain Name
11. FTP : File Transfer Protocol
12. GB : Gigabyte
13. GHZ : Gigahercio
14. GID : Group Identifier
15. GPO : Group Policy Object
16. HD : Hard Disk
17. HTML : Hypertext Markup Language

18. IDMAP : Identity Mapping
19. IP : Internet Protocol
20. ISP : Internet Service Provider
21. KDC : Key Distribution Center
22. LAN : Local Area Network
23. LDAP : Lightweight Directory Access Protocol
24. Mb : Megabits
25. Mbps : Megabits Por Segundo
26. NTP : Network Time Protocol
27. OU : Organizational Unitphp
28. RAM : Random-Access Memory
29. SID : Security Identifier
30. SMB : Server Message Block
31. SO : Operating System
32. TCP : Transmission Control Protocol
33. TI : Technology Infrastructure
34. UDP : User Datagram Protocol
35. UID : User Id
36. WAN : Wide Area Network

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

CAPÍTULO 1

1. Análisis de la infraestructura de TI

1.1. Introducción

Las empresas en la actualidad apuntan a la seguridad de la información, sin que esta deje de ser accesible para los usuarios. Para hacer esto posible existen estándares internacionales como la serie de normas **ISO/IEC 27000**. En esta familia una de las más importantes es la **ISO/IEC 27001**, que menciona la importancia de contar con un sistema de gestión de seguridad de la información (SGSI). Este sistema adapta políticas, para de esta manera tener una mejor organización del diseño, implantación, y mantenimiento de un conjunto de procesos para gestionar eficientemente la accesibilidad de la información, buscando asegurar la confidencialidad, integridad y disponibilidad de los activos de información minimizando a la vez los riesgos de seguridad de la información.

Entre los objetivos de control que cita el estándar ISO/IEC 27001, y en los que basaremos nuestra solución se encuentran el anexo **A.11.1**

el control de acceso a la información, en el anexo **A.11.2** asegurar el acceso del usuario autorizado, y evitar el acceso no autorizado a los sistemas de información, el anexo **A.11.6.2,** que hace mención sobre el aislamiento de los sistemas e información sensible en ambientes diferentes.

También existe una estrategia de mejora continua en las empresas conocida como el circulo **PDCA** (Planificar, Hacer, Verificar, Actuar), la implementación de esta da como resultado una mejora integral de la competitividad, de los servicios e información importante para la empresa, mejorando continuamente la calidad, reduciendo costos, optimizando la productividad y por ende, mejorando la rentabilidad.

Basados en estos estándares y utilizando las herramientas de código abierto disponibles, implementaremos una solución que permita manejar información de forma íntegra con la mayor disponibilidad y confidencialidad posible a fin de contar con una herramienta a considerar en una futura certificación internacional para la empresa.

1.2. Objetivos Generales

Facilitar el acceso y la compartición de la información entre usuarios de diferentes plataformas tecnológicas como son Windows y Linux, a fin de otorgar facilidades en el intercambio de información de manera confiable y segura.

1.3. Objetivos Específicos

- Analizar la infraestructura de TI a ser considerada en la compartición de recursos entre usuarios Windows y Linux.
- Identificar la arquitectura, herramientas y protocolos a ser empleados para la implementación de la solución.
- Diseñar una arquitectura de TI basada en Linux para hacer posible la compartición de recursos de diferentes plataformas.
- Implementar una solución tecnológica escalable, compatible con Windows y Linux, para la compartición de recursos entre estas dos plataformas.

1.4. Análisis de Infraestructura LAN

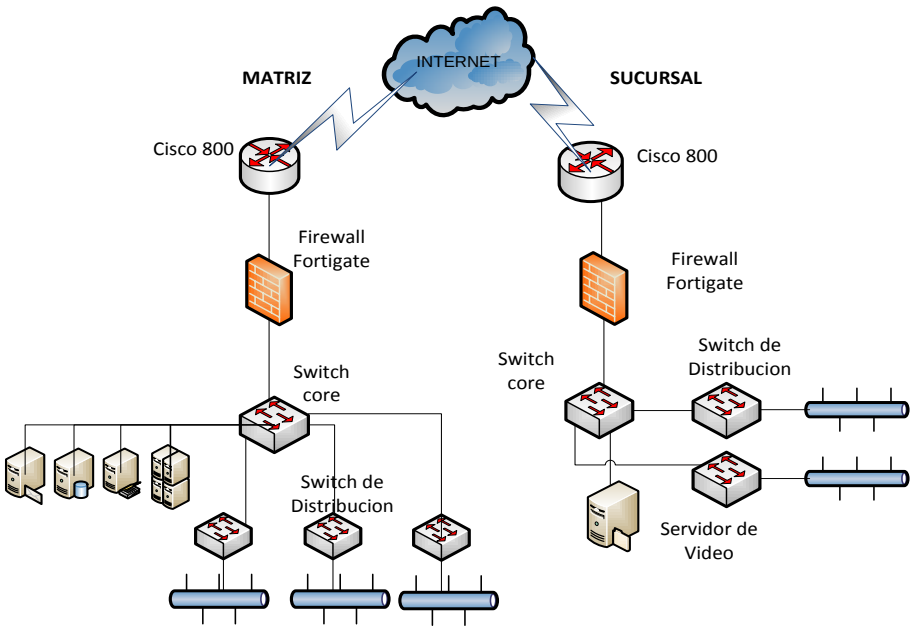

Figura 1.1 Diagrama de la Infraestructura TI

La empresa ha estado inmersa en un cambio de tecnología en los últimos meses, esto debido al crecimiento de la misma y al mercado que requiere de su funcionalidad al cien por ciento. Uno de los cambios realizados fue contratar a una empresa externa para que realice el cableado horizontal, con la debida certificación de los puntos, tanto en la matriz como en la sucursal.

1.4.1. Acceso a Internet

Como se muestra en la Figura 1.1, En la matriz situada en la ciudad de Guayaquil se cuenta con un enlace a internet de 6Mb compartición 1:1. El internet llega por un enlace de radio, el mismo que es utilizado para una conexión de datos arrendada a la ciudad de Quito. El servicio llega a un equipo modulador CFM-M4-MUX, una vez que la señales modulada se conecta a un puerto FastEthernet WAN en un router cisco 800, es en este equipo donde el enlace de datos hacia la ciudad de quito y el internet salen por diferentes puertos. Hasta el router cisco 800 los dispositivos son propiedad del ISP.

En la sucursal la topología es similar a la matriz, se tiene un enlace de datos contratado 2 Mb y conexión a internet de 2.5 Mb que salen por diferentes puertos del router cisco 800 que es propiedad del proveedor. Se cuenta con un firewall

Fortigate donde están implementadas las reglas de navegación. Enlace de datos con la matriz es requerido para la funcionalidad del active directory, el correo y las aplicaciones que la empresa maneja. En la sucursal hay 40 puntos de datos certificados de categoría 6. Para los puntos de datos se cuenta con 2 switch de 24 puertos ubicados en el rack de comunicaciones.

1.4.2. Seguridad lógica en la empresa.

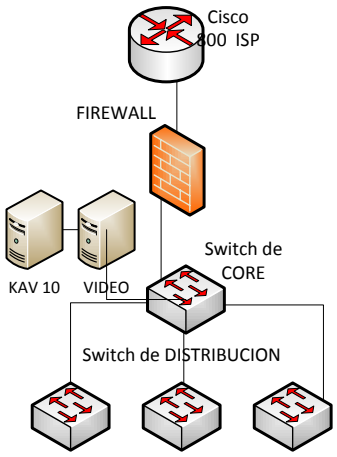

Figura 1.2 Topología de seguridad

La empresa posee un firewall Fortigate 60C en la matriz así como en la sucursal, es aquí donde se aplican políticas de navegación y políticas de seguridad. Conectado por medio de un puerto WAN se encuentra el switch principal que es de 24 puertos, es en este switch es donde están conectados 2 switch en cascada de 24 puertos y otro por medio de un enlace de

fibra óptica también de 24 puertos. Los 3 switch son de acceso para 62 puntos de datos certificados.

También se cuenta con un servidor de antivirus Kaspersky el mismo que tiene instalado un agente en cada computador de la empresa, para el control y prevención de ataques internos y externos a los datos de la empresa. Para la seguridad física se cuenta con cámaras de video que cubren los lugares más delicados de la empresa. Las cámaras utilizan el protocolo TCP para su funcionamiento. Para el almacenamiento del video y el control de las mismas se cuenta con un servidor de video. El área de administración donde está ubicado el rack de comunicaciones cuenta con alarma privada para mayor seguridad. Además de esto la empresa cuenta con un control de guardianía las 24 horas, para el control del acceso a la empresa.

1.4.3. Infraestructura LAN

El cableado en su totalidad es de categoría 6. La máxima distancia entre departamentos es de 120 metros. Entre el departamento de cobranzas y el departamento de administración se colocó un enlace de fibra óptica multimodo ya que la distancia entre estos así lo demando.

1.4.3.1. Servidores, servicios y estaciones de trabajo

La empresa tiene los siguientes servidores y servicios:

Servicio	SO	Características
Active directory – Exchange	Windows Server 2008 R2	24 Gb RAM 4TB HD Virtualizado Vware 4.5
Aplicaciones – Base de datos	Windows Server 2008 R2	12 Gb Ram 1 TB HD
Antivirus	Windows 8	500 GB DE HD
FTP	Windows 7	2 TB 8 GB de RAM
Video Matriz	Windows 7	8 GB de RAM
Video Sucursal	Windows 7	8 GB de RAM

Tabla 1.1 Servicios y servidores

Para el dominio seei.com se cuenta con un servidor Windows server 2008 r2, el mismo que está ubicado en la matriz y alberga a todos los usuarios de la empresa, se tienen implementadas OU por cada departamento, y GPO para cada localidad. Los usuarios de la sucursal se autentican en el DC ubicado en la matriz, esto por medio de un enlace de datos arrendado.

La empresa maneja un ERP para el control centralizado de la información de los diferentes departamentos. Este sistema se encuentra virtualizado en un servidor Windows Server 2008 R2, para esto cuenta con vware 4.5.

1.4.3.2. Detalles de las estaciones de trabajo

Tipo	WorkStation	Laptop
porcentaje	20%	80%
Sistema	Windows 7 de 64 bits *Service Pack 1*	
Procesador	>= Intel Core 2 Duo 2.5 Ghz	>= Intel Core 2 Quad
Memoria	>= 2,00GB Ram	>= 2,00GB Ram
Disco duro	500 GB SATA	500 GB SATA
Tarjeta de Red	Intel Pro10/100/100 Mbps.	Intel 82566 10/100/100

Tabla 1.2 Detalle de las Estaciones de trabajo.

En estaciones de trabajo la matriz tiene 60 computadores, y la sucursal cuenta con 48 mayoritariamente laptops. Los equipos tienen instalado Windows 7 profesional de 64 bits con licencia original. Las características de los equipos son acorde a la tecnología actual, Un 80 % tiene un procesador superior a core 2 duo, memoria de 2 GB y disco duro de 500GB.

Todos los computadores están dentro del dominio seei.com, en cada computador hay 3 usuarios: el administrador local, el administrador del dominio, y un usuario que esta creado dentro del dominio.

Debido a que la mayoría de usuarios utilizan laptops, en cada departamento hay un AP que cubre al 100% la cobertura de dicho departamento, como redundancia cada laptop tiene un cable de red disponible en el caso de que la red inalámbrica falle.

1.5. Análisis de Infraestructura WAN

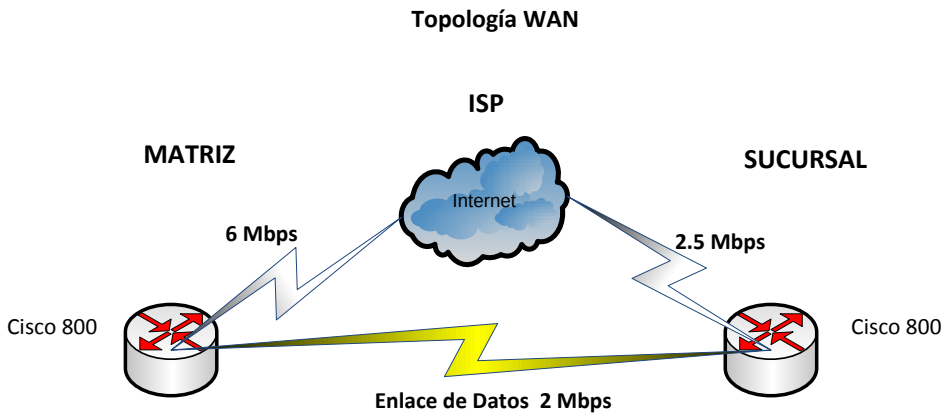

Figura 1.3 Análisis de la Topología WAN

La infraestructura WAN de SEEI está compuesta por enlaces a internet en el caso de la matriz con un canal de 6Mbps para el acceso a internet, y en el caso de la sucursal un canal de 2.5 Mbps para el

servicio de internet. Adicional a esto se tiene un enlace de datos arrendado para el acceso de la sucursal a los diferentes servicios ubicados en la matriz.

1.6. Análisis de plataformas Windows - Linux

1.6.1. Análisis de la plataforma Windows

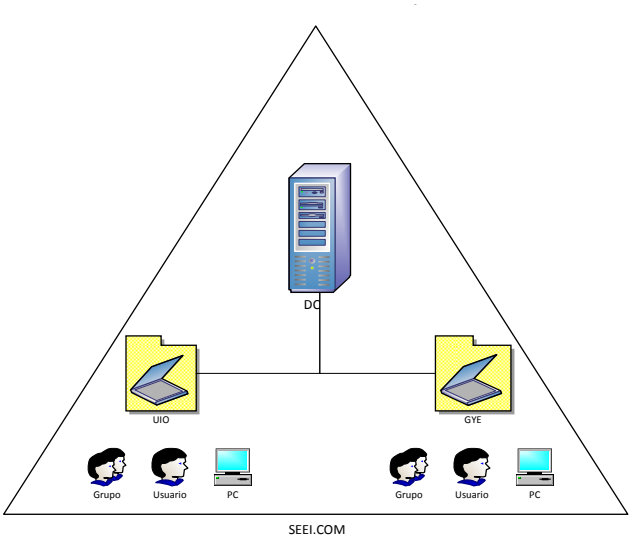

Figura 1.4 Estructura del Active Directory

La estructura de active directory en la empresa SEEI como se muestra en la Figura 1.4, consta de un único bosque con un single domain, el forest root domain está ubicado en la matriz de la empresa y es donde se encuentran creados los diferente OU con sus respectivas políticas.

En la empresa todas las computadoras están unidas al dominio seei.com. En la sucursal se utiliza el enlace de datos hacia la matriz para que los usuarios puedan autenticarse y tener

acceso a los diferentes repositorios de recursos compartidos e impresoras dentro del dominio.

Los usuarios que se encuentran en la sucursal hacen la consulta dns en el domain controller. Debido a que existe un solo dominio y la cantidad de usuarios es pequeña, también hay un solo site para el dominio.

1.6.2. Diseño de la Unidad Organizativa

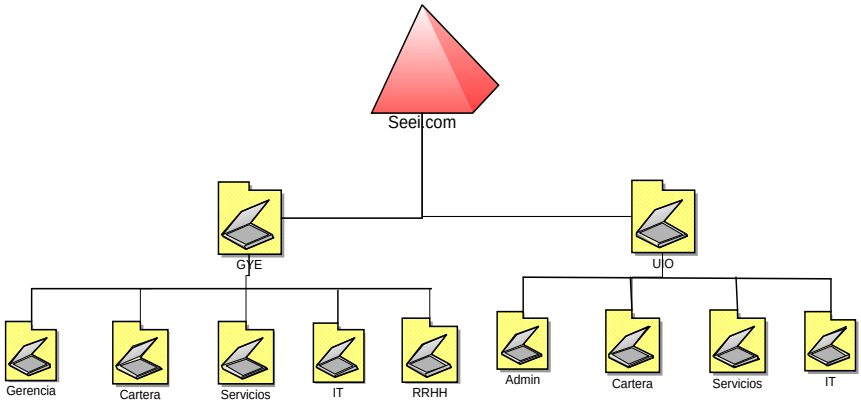

Figura 1.5 Estructura OU

La estructura OU de la organización tiene un modelo hibrido de ubicación, entonces organización, ya que es el modelo más adecuado para nuestro caso.

En el estudio realizado se muestra que puede darse el caso de que un departamento puede cambiarse de piso. Por tal motivo y otros hemos implementado este modelo.

En cada departamento se encuentran:

Usuarios, computadoras, grupos, impresoras, aplicaciones, políticas de seguridad, carpetas compartidas, otras OU. Los cuales requieren permisos administrativos diferentes en cada departamento.

Con este diseño podemos delegar control administrativo de objetos a cada departamento, así como también establecer los límites de visibilidad de objetos y controlar las aplicaciones del Group Policy.

CAPÍTULO 2

2. Diseño de la solución

2.1. Diseño de infraestructura TI.

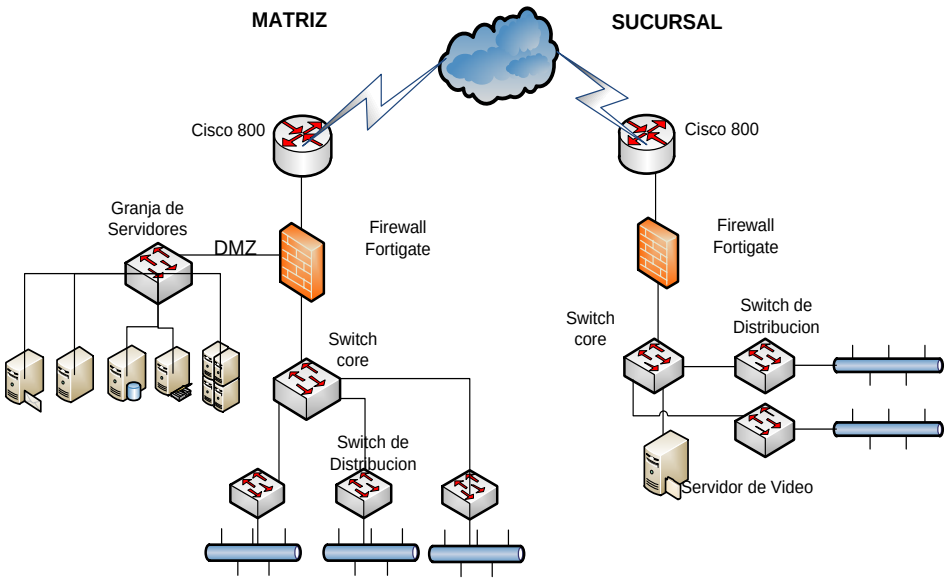

Figura 2.1 Diseño de la infraestructura TI

Como podemos ver en la Figura 2.1, en la topología de TI, por motivos de seguridad se ha implementado una DMZ, donde se encuentra la granja de servidores, incluida la nueva plataforma Linux. En lo que al

cableado se refiere, no se harán cambios ya que este fue implementado y certificado recientemente.

2.2. El directorio Activo

2.2.1. Plan de bosque

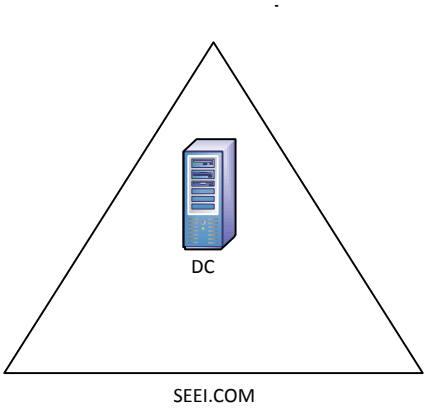

Figura 2.2 Plan de bosque

En el diseño del forest para la empresa SEEI, se mantiene el plan de bosque, esto debido a que existe una sola empresa sin relaciones de confianza con otro forest root domain. A más de esto la administración se mantiene de forma centralizada y simplificada en la matriz.

2.2.2. Plan de Dominio

El único dominio que posee la empresa, como se muestra en la Figura 2.2 no se verá modificado ya que funciona de manera eficiente y la estructura que tiene cumple con los requerimientos de replicación y la capacidad existente de la

infraestructura de red. Este dominio es declarado en la plataforma de Linux para interactuar y llevar a cabo las funciones de interoperabilidad y compartición de archivos entre las dos plataformas.

2.2.3. Estructura del modelo OU

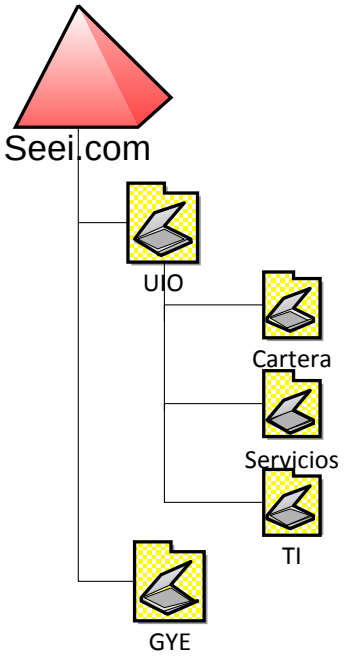

Figura 2.3 Estructura del modelo OU

La empresa posee una estructura de OU hibrido de ubicación entonces organización, que representa la ubicación geográfica y un bajo nivel de OU basado en la organización, este modelo nos permitirá adicionar departamento y divisiones en crecimiento incluso podemos aglomerar usuarios determinados a los cuales tendrá acceso la nueva plataforma.

2.2.4. Plan de espacio de nombres DNS

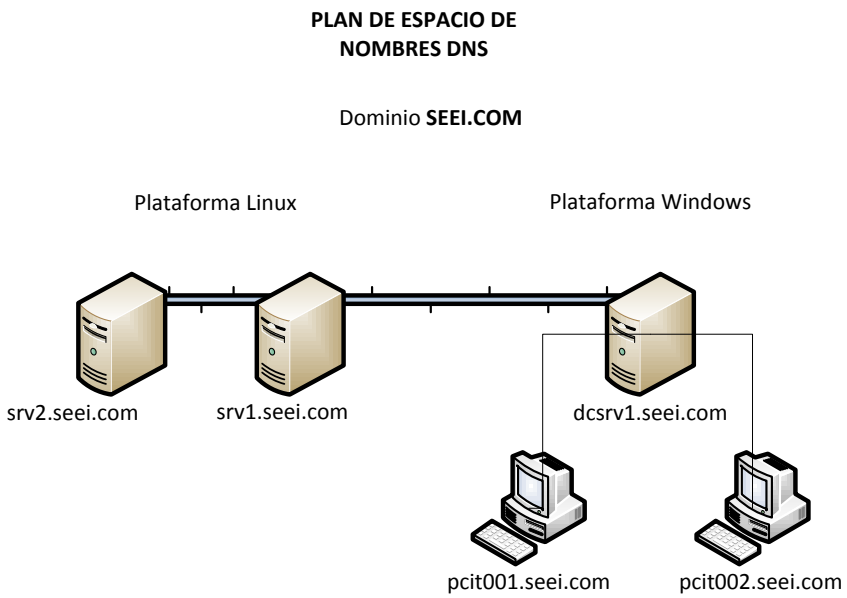

Figura 2.4 Plan de espacios de nombres DNS

Para la plataforma Windows no se ha modificado el plan de espacio dns como se muestra en la Figura 2.4, quedando el dns domain como: **seei.com**, para el servidor DC, el FQDN seria; **dcsrv1.seei.com**. Para las maquinas estaciones en la plataforma Windows el FQDN es: **pcit001.seei.com** **pcit002.seei.com**. Etc.

El espacio de nombres DNS para la nueva plataforma linux implementada se identifica de la siguiente manera. Servidor Principal: **srv1.seei.com**. Servidor secundario de la plataforma Linux: **srv2.seei.com**.

El espacio de nombres DNS para el ingreso vía web se define en el servidor Linux principal como: **file.srv1.seei.com** y en el servidor secundario como **file.srv2.seei.com**.

2.3. Enlace al dominio

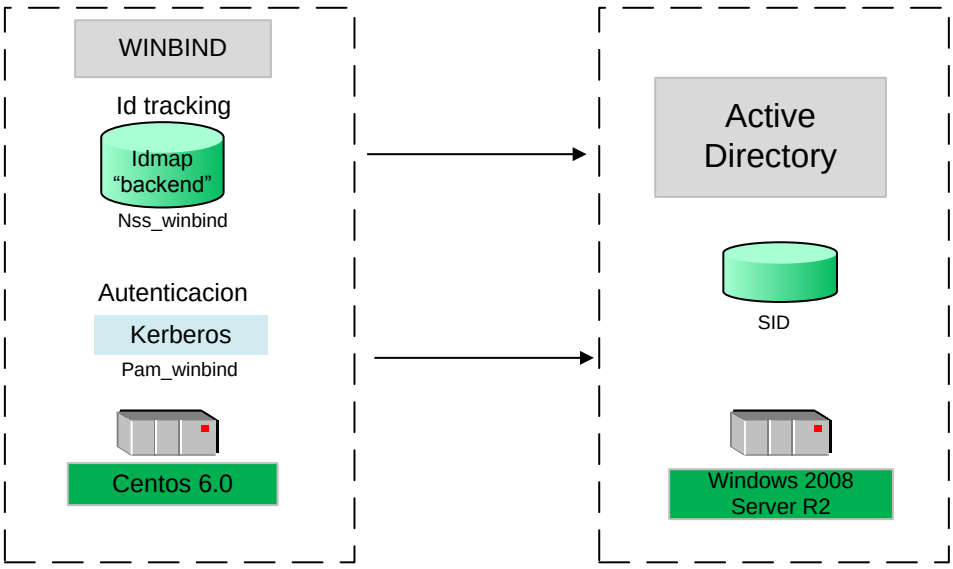

Figura 2.5 Enlace al dominio

La plataforma Windows que consta en el diseño de la implementación consta de un sistema operativo Windows 2008 Server R2 que hace de Domain Controller, sobre esta plataforma reposa un active directory que asigna un SID (Security ID) de forma automática a objetos de la entidad principal de seguridad en el momento de su creación. Las entidades principales de seguridad son cuentas de Active Directory a las que se pueden asignar permisos, como por

ejemplo, las cuentas de equipo, grupo o usuario. Una vez emitido un SID para el usuario autenticado, se adjunta al ticket de acceso del usuario.

En la plataforma Linux se encuentra instalado un Centos 6.0 y este al igual que Windows utiliza un UID (User ID o ID de usuario) para identificar al usuario particular. Y el GID (Group ID o ID de grupo) se utiliza para identificar a un grupo. Dentro del sistema Linux el usuario puede pertenecer a muchos grupos secundarios y cada grupo secundario tendrá un GID único.

Mediante la configuración de los protocolos como Kerberos y DNS el manejo del ID del usuario y del logon entre ambas plataformas será a través de Winbind, un componente de SAMBA que simplifica la configuración y manejo de los métodos de autenticación del usuario Linux permitiendo a un usuario del Servicio de Dominio Active Directory de Windows integrarse y operar con un usuario local de Linux.

2.4. Diseño del entorno Web.

2.4.1. Interfaz de login

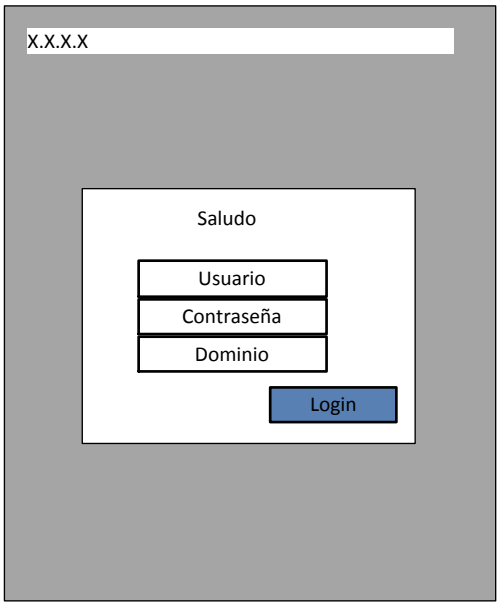

Figura 2.6 Pantalla de login

En la Figura. 2.6 se muestra la interfaz de Login que tendrá la herramienta, en esta interfaz se mostrará un saludo y los campos de usuario, contraseña y nombre de dominio o dirección IP del servidor, por defecto se mostrara el nombre de dominio en donde se encuentra alojada la aplicación. La autenticación se realizara contra el servidor al cual se desea acceder mediante la aplicación web una vez presiona el botón de Login. Contará con las debidas validaciones en los campos y restricciones dependiendo del usuario que accede.

2.4.2. Modulo principal Host.

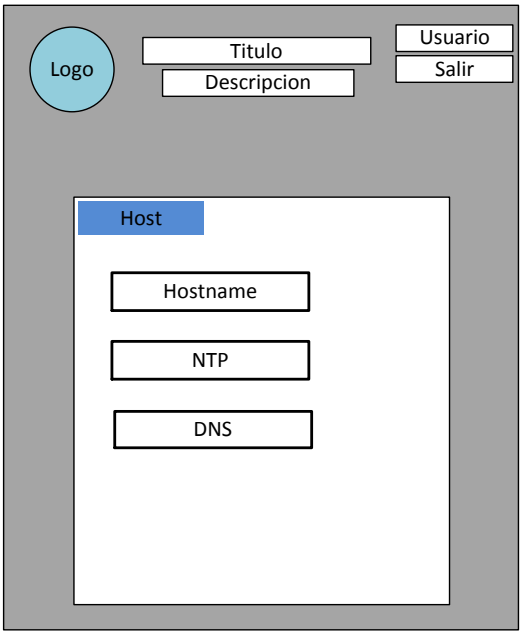

Figura 2.7 Modulo de Host

En la Figura 2.7, la interfaz principal denominada host, se muestra información básica del servidor y se permite su configuración para la previa integración al dominio Windows. Esta interfaz tendrá 3 secciones de configuración:

Hostname.- Se mostrara el nombre actual del servidor al cual ingresamos, su dirección IP y un campo donde debemos ingresar el nombre de dominio en formato FQDN que tendrá el servidor para integrarse al dominio Windows.

NTP.- Me permitirá ingresar una dirección IP o el nombre de dominio en formato FQDN del servidor NTP con el que se sincronizara el reloj del servidor.

DNS.- En este campo se deberá ingresar la IP del servidor DNS del dominio con el que se está realizando la integración.

2.4.3. Modulo autenticación

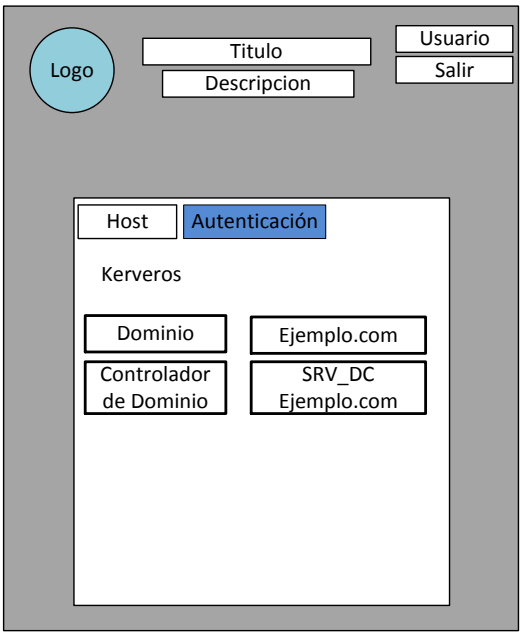

Figura 2.8 Modulo de autenticación

El módulo de autenticación deberá permitir configurar el servidor de autenticación del dominio al cual se desea enlazar, todo se realizara de una manera transparente para el usuario. En el campo dominio se deberá ingresar el dominio Windows y en el campo controlador de dominio ingresaremos el nombre de

dominio en formato FQDN del servidor encargado de la autenticación.

Una vez ingresado los datos y realizada la configuración se enviara al usuario a la siguiente interfaz de configuración.

2.4.4. Módulo Integración

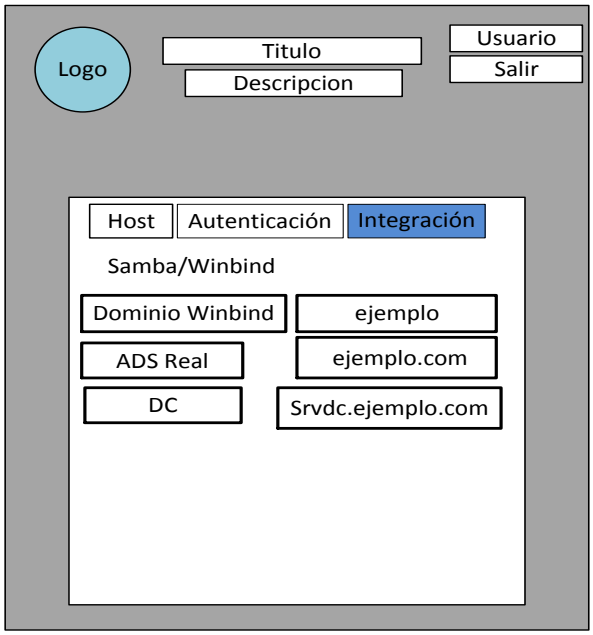

Figura 2.9 Modulo de Integración

En el módulo integración se habilitara la autenticación de usuarios del dominio Windows dentro de la plataforma Linux y se integrara el servidor dentro del dominio. En el campo Dominio Winbind, ingresamos nombre del dominio en un segundo nivel. En ADS Realm ingresamos el dominio DNS y en DC ingresamos el nombre de dominio FQDN del controlador de

dominio. De esta forma y de manera transparente para los usuarios se configura y levanta los servicios necesarios para integrar el servidor al dominio.

2.4.5. Módulo de información

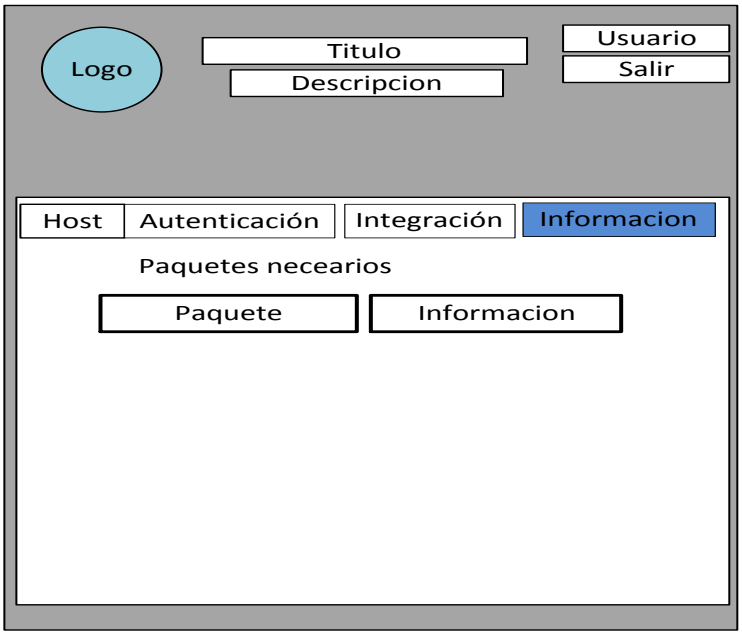

Figura 2.10 Modulo de información

En este módulo se debe mostrar información de los paquetes necesarios para la correcta integración del servidor al dominio Windows, así como también la posibilidad de mostrar si un paquete no está instalado y proceder a la instalación del mismo, también Permitirá monitorear el acceso a los recursos

compartidos por el servidor mientras se encuentra en este módulo, capturando los sucesos en un archivo de logs.

2.4.6. Módulo de servidores.

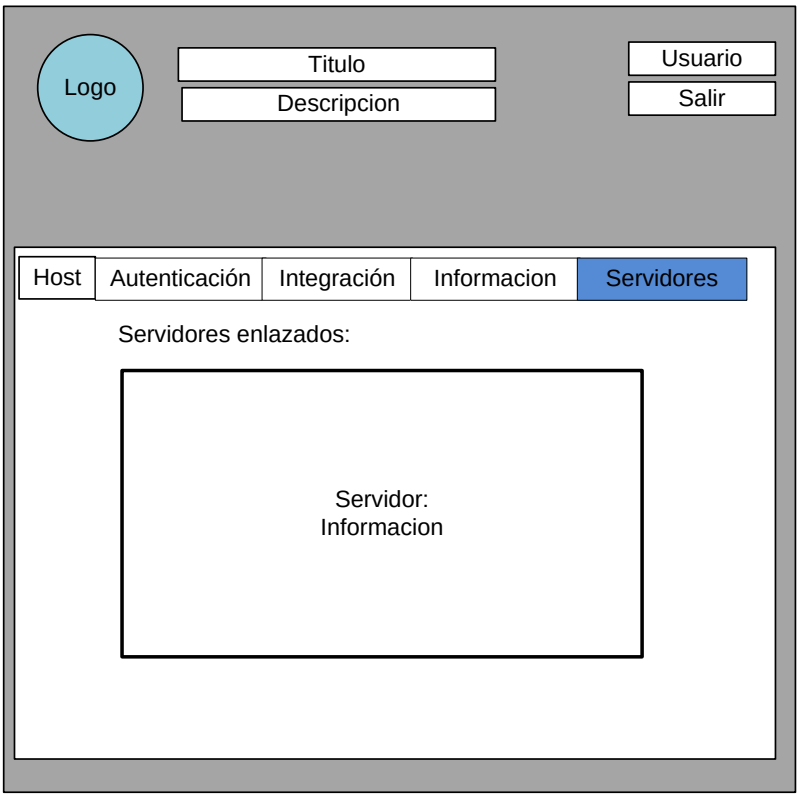

Figura 2.11 Modulo de servidores

Dentro de este módulo podremos tener acceso a la información de los servidores que han sido enlazados con éxito a un Dominio Windows. Se mostrara información del host tal como dirección IP que le pertenece, nombre de dominio con el cual está configurado, Información del dominio con el cual se

encuentra enlazado, Datos de configuración de autenticación, integración, servidores NTP y servidores DNS configurados.

CAPÍTULO 3

3. Implementación de la solución

Es necesario conocer el funcionamiento de las plataformas entre las cuales se desea crear una interoperabilidad mediante los servicios y protocolos que se pueden emplear para entablar una comunicación mutua entre plataformas, es por eso que se detallan desde el siguiente tema los factores que entran en juego para obtener este nivel de integración.

3.1. Plataforma Windows

Windows server 2008 que está basado en Windows NT 6.1, pertenece a la familia de sistemas Windows desarrollados y distribuidos por Microsoft, puede ofrecer una gran cantidad de servicios de red empleando estándares y protocolos propios de Microsoft.

El servicio Active Directory que tiene como complemento permite la creación de un dominio Windows dentro del cual se tiene una total administración de los dispositivos, usuarios y recursos que existen en la red y un control mediante la creación de grupos y políticas de

seguridad. La organización jerárquica de todos los recursos ofrece una gran escalabilidad del servicio mediante la expansión y enlace con otros dominios. Por este gran motivo Windows server se ha posicionado de gran manera en las empresas en donde la organización jerárquica y total administración de sus recursos de TI es algo de gran importancia.

Este será el sistema con el cual se realizara la integración.

3.2. Plataforma Linux

Linux es un sistema operativo basado en Unix con licencia GPL se encuentra empaquetado en varias formas llamadas distribuciones. Red Hat Enterprise Linux; distribución comercial es un sistema empresarial que ofrece soporte y gran estabilidad en sus productos.

CentOS es la distribución compilada desde los códigos fuentes liberados por Red Hat Enterprise Linux, ofrece a los usuarios un sistema operativo empresarial y estable sin la necesidad de pagar por un soporte para acceder a sus beneficios, es por este motivo que es muy empleado en el entorno de servidores y será nuestra plataforma de desarrollo para el proyecto de integración.

3.3. Protocolos y servicios que intervienen

3.3.1. Servicio de Directorio Activo

Servicio de Directorio Activo o Active Directory Service una herramienta de Microsoft que se encuentra repartida en uno o varios servidores dentro del dominio Windows y permite la creación equipos, usuarios y grupos como objetos dentro de dicho dominio. Toda la información de la organización de los objetos se encuentra en una base de datos central la cual puede ser replicada en todo el dominio y a la cual se puede acceder en busca de información sobre un objeto. Cada objeto es único y tiene características que pueden identificarlo como unívoco, lo cual permite la aplicación de políticas de seguridad, control y administración.

Para esto hace el servicio de Active Directory hace uso principalmente de los protocolos:

- Lightweight Directory Access Protocol (LDAP) es una versión modificada por Microsoft de Kerberos
- Domain Name System (*DNS)*

3.3.2. Lightweight DIrectory Access Protocol

Lightweight Directory Access Protocol o Protocolo Ligero de Acceso a Directorios es un protocolo a nivel de aplicación que permite el acceso a un servicio de directorio en busca de información a través del Protocolo de Internet IP.

Un cliente LDAP inicia una sesión conectándose a un servidor LDAP mediante el puerto 359 en TCP y UDP, él cliente envía una petición y el servidor envía una respuesta. No es necesario que el cliente reciba una respuesta para enviar otra petición.

Además de realizar consultas permite actualizar la información sobre los objetos del directorio y comúnmente es empleado para realizar una sola autenticación basada en usuario y contraseña del cliente, la cual es compartida entre varios servicios para validar el acceso a estos.

3.3.3. Kerberos.

Es un protocolo de autenticación en red que permite que los dispositivos que se encuentren conectados a esta puedan demostrar su identidad de manera segura mediante “tickets”, brinda autenticación mutua, tanto el cliente como el servidor pueden demostrar su identidad.

Kerberos está basado en un método criptográfico en el cual emplea una única clave para cifrar y descifrar mensajes; y un mediador de confianza llamado Key Distribution Center el cual

está formado lógicamente por el Authentication Server y el Ticket Granting Serve.

Los mesajes de kerberos están protegidos mediante cifrado y los equipos que realicen una autenticación mediante Kerberos deben tener sincronizados sus relojes.

3.3.4. Network Time Protocol

Network time Protocolo o NTP es un protocolo de red que permite sincronizar los relojes de los dispositivos conectados en red a través de enrutamiento de redes con latencia variable.

El protocolo se describe como un modelo cliente servidor pero puede emplear un modelo peer-to-peer en donde ambos peers consideran al otro como una potencial fuente de tiempo para sincronización. Emplea un sistema jerárquico de estrato de relojes empezando desde 0, estos sinconizan a los de estrato 1 y estos pueden sincronizarse entre si y asi sucesivamente hasta llegar al 16.

NTP envía y recibe timestand atreves del puerto 123 en UDP, también puede usar broadcasting o multicasting, los clientes esperaran actualizaciones después de una ronda de calibración

3.3.5. Domain Name System

Sistema de Nombres de Dominio o DNS es un sistema de nomenclatura jerárquica para cualquier dispositivo o recurso conectado en red. Este asocia información variada sobre el dispositivo con su nombre de dominio y cuya función principal es traducir los nombres de dominio en una dirección IP para poder localizar al dispositivo o recurso conectado en red de manera local o mundial a través de Internet.

El espacio de nombres de dominio consiste en un árbol de nombres de dominio, en el cual cada hoja posee mas recursos o nada. El árbol se subdivide en una zona root y en una zona DNS, que puede consistir de un dominio o de muchos dominios y subdominios. Dependiendo de la autoridad administrativa.

3.3.6. Server Messages Block

El Server Message Block o SMB es protocolos de red que permite la compartición de recursos tales como archivos e impresoras entre los nodos de una red, fue desarrollado por IMB y es usado en los sistemas Windows. Microsoft luego de realizar algunas modificaciones lo renombro a Common Internet File System o CIFS.

SMB trabaja mediante el modelo cliente-servidor, una parte del protocolo SMB se encarga del acceso al sistema de archivos, cuando el cliente realiza peticiones al servidor de archivos; otra parte del protocolo se encarga del Inter-Process Communication que permite el intercambio de datos entre múltiples hilos de uno o más procesos los cuales pueden ejecutarse en uno o múltiples equipos a las vez conectados a la red. Emplea el puerto:

- 445 sobre TCP
- vía NetBIOS
    - puerto 137, 138 sobre UDP y puerto 137, 139 sobre TCP
    - Sobre varios protocolos heredados como NBF

Permitir a los clientes al acceso a los archivos e impresora que se encuentra en el servidor SMB, es la función principal por la cual es empleado. Todas las implementaciones de los servidores SMB emplean la autenticación del dominio NT para validar el acceso a los recursos.

3.3.7. Samba

Es una suite de programas que permiten la implementación del protocolo de red SMB/CIFS para los sistemas Unix, de esta

manera es posible que los sistemas Linux interactuar con sistemas Windows compartiendo o accediendo a recursos.

Fue desarrollado por Andrew Tridgell mediante ingeniería inversa e implementa una docena de servicios y protocolos tales como:

- NetBIOS sobre TCP/IP (NetBT)
- SMB /CIFS
- Microsoft Remote Procedure Call (MSRPC)
- WINS, conocido como el servidor de nombres NetBIOS (NBNS)
- Suite de protocolos del dominio NT, con su Logon de entrada a dominio
- Base de datos del Security Accounts Manager (SAM)
- Local Security Authority (LSA)
- Servicio de impresoras de NT y el Logon de entrada de Active Directory, con una versión modificada de Kerberos y del LDAP
- NetBIOS y WINS ya no son usados por Windows.

  Samba implementa sus servicios mediante dos demonios dentro del sistema Unix:

- smbd, que permite la compartición de recursos

- nmbd, que permite el servicio NetBIOS sobre TCP/IP

El acceso de los usuarios a los recursos compartidos mediante samba depende del nivel de seguridad con la que se configura Samba, tal nivel indica contra quien se realizara la autenticación de los usuarios para la cual puede ser local o externa; contra otro servicio Samba o Servicio Active Directory, este último se logra mediante el uso de Winbind.

3.3.8. Winbind

Winbind es componente de samba que resuelve los problemas de la unificación de logon del usuario mediante la implementación de Microsoft Remote Procedure Call (MSRPC), Pluggable Authentication Modules (PAMs) y el Name Service Switch (NSS); empleado por defecto cuando winbind no es usado, esto permite a un usuario de Dominio Windows integrarse y operar como un usuario del Sistema tipo Unix.

3.3.9. Microsoft Remote Procedure Call

Es una versión modificada por Microsoft del protocolo DCE/RPC que es el sistema de llamada a procedimiento remoto desarrollado para el entorno de la informática distribuida, esto permite la ejecución y transferencia datos

entre las partes de un programas distribuido que se encuentra en varios equipos.

3.3.10. Pluggable Authentication Modules

El pluggable authentication module o PAM es un mecanismo de autenticación en que integra múltiples autenticaciones de bajo nivel dentro de una API de alto nivel, permitiendo a los programas que requieren de autenticación utilizar y emplear varios métodos de autenticación, para que de esta manera no tener que escribir un código específico para realizarlo.

3.3.11. Name Service Switch

El Name Service Switch o NSS es un mecanismo de los sistemas tipo Unix para utilizar varias fuentes para la resolución de nombres y contraseñas, como archivos propios del sistema (/etc/passwd, /etc/group, /etc/hosts,), DNS, LDAP o NIS.

El NSS se puede configurar mediante el archivo /etc/nssswitch.conf, en donde se encuentra una lista de bases de datos como passwd shadow y group además

de otrar fuentes de información como archivos locales, LDAP.NIS. NIS+ y WINS.

3.3.12. Network Information Service

Servicio de información de red o NIS es un protocolo de servicios de directorio cliente-servidor que envía datos de configuración en sistemas distribuidos como nombres de usuarios y host entra los equipos de una red.

Agrega una nueva lista de usuarios global, la cual es usada para autenticar usuarios en cualquier cliente del dominio NIS.

El NIS distribuye y mantiene un directorio central de usuarios, grupos, hostnames, correos y otra información sobre una red,

3.4. Introducción de Integración al dominio

Winbind es un componente clave para el manejo de la integración y de la interoperabilidad entra las plataforma. Este unifica la administración de las cuentas Linux y Windows mediante la conversión de un sistema Linux en un miembro completo de un dominio Windows, después de realizada esta acción los usuarios del dominio pueden actuar de manera nativa dentro del sistema Linux.

La arquitectura cliente-servidor con la que fue desarrollada hace que el demonio winbindd este en espera de peticiones generadas vía NSS o PAM, las cuales son resueltas de manera secuencial. El funcionamiento es de la siguiente manera y se encuentra dividido en tres tareas:

- ✓ Mediante el empleo de MSPRC puede recoger información de usuarios y grupos, autenticar usuarios o realizar cambios en la información de los usuarios dentro de un dominio Windows y realiza un *ID mapping* de la cuenta de dominio dentro del sistema Linux.
- ✓ Vía NSS puede presentarse como un proveedor de información cuando el sistema Linux resuelve nombre de usuarios y grupos y genera un *ID Tracking* que determina donde fue identificado el usuario.
- ✓ Empleando PAM permite que los login de usuarios de dominio Windows en los sistemas Linux se autentiquen contra un PDC, Winbind se integra a PAM mediante el modulo pam_winbind.so; como un servicio que requiere de autenticación.

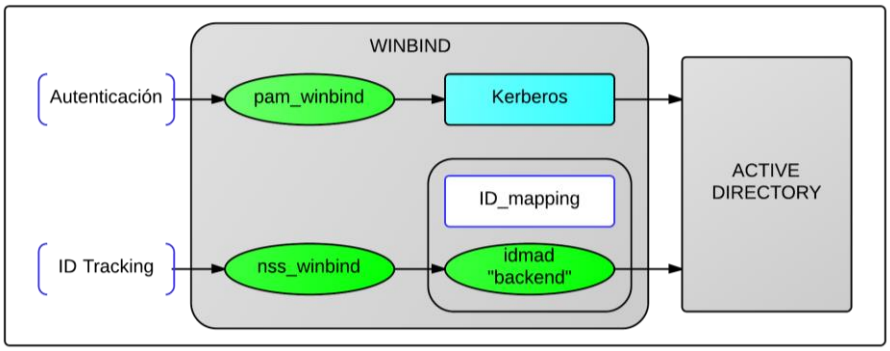

Figura 3.1 Funcionamiento de Winbind

3.4.1. ID mapping

El ID mapping que ofrece Winbind puede ser manejado mediante el uso de diferentes idmap “backends”, cada uno maneja el ID mapping de diferente manera, se pueden clasificar de la siguiente manera:

- ✓ Allocating - “Read-Writeable” el ID mapping es almacenado en una base de datos local dentro del sistema Linux.
- ✓ Algorithmic - “Read-Only” el ID mapping es calculado y ofrece un consitente ID mapping en todos los distemas Linux.
- ✓ Assigned - “Read-Only” utiliza un ID mapping pre-configurado por el Active Directory.

El backend idmap_rip es un backend de tipo Algorithmic - “Read-Only” cuyas características son la siguiente:

- ✓ Algoritmo de ID mapping rapido a través de múltiples servidores
- ✓ Requiere configuración adicional para soportar un Forest de múltiples Dominios AD o múltiples Domains trees.

3.5. Despliegue de la integración Windows – Linux

Una vez entendido los distintos servicios y protocolos que entran en juego entre las dos plataformas para poder compartir información y recursos entre sí, se pueden explicar cuáles con los pasos a seguir para logar dicho objetivo.

3.5.1. Servidor Windows

Dentro del Windows server 2008 R2 ya se encuentra implementado el dominio **seei.com**, en el cual cumple el rol de PDC, servidor DNS, servidor de autenticación y servidor NTP, con un nombre de dominio **dcsrv1.seei.com** y dirección IP 192.168.0.100**,** por lo cual no necesita mayor configuración.

3.5.2. Servidor Linux

Dentro del servidor CentOS 6.0 cuya dirección IP es 192.168.0.200 se deberá realizar la siguiente pre configuración.

El nombre del sistema deberá ser cambiado al formato FQDN del dominio al cual se desea integrar. Se debe editar el archivo /etc/sysconfig/network y cambiar la línea HOSTNAME. Una vez hecho el cambio se deberá reiniciar para que el cambio tenga resultado.

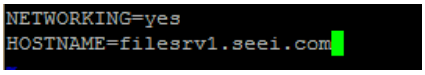

Figura 3.2 establecer nombre de dominio

3.5.2.1. Sincronización de reloj

Es necesario que el reloj del servidor este sincronizado con el reloj del servidor de dominio Active Directory, de otra manera el desfase existente producirá una falla en la autenticación mediante Kerberos, para esto se realizaran los siguientes pasos:

- Agregar el servidor ntp del dominio al archivo de sincronización */etc/ntp.conf.*

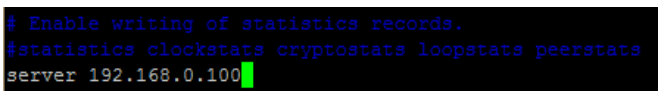

Figura 3.3 Agregar servidor NTP

- Detener el servicio ntpd, actualizar el reloj con el servidor ntp del dominio e iniciar el servicio nuevamente

```
[root@filesrv1 ~]# service ntpd stop
Shutting down ntpd:                                        [  OK  ]
[root@filesrv1 ~]# ntpdate 192.168.0.100
 1 Feb 06:12:54 ntpdate[1866]: adjust time server 192.168.0.100 offset 0.001441 sec
[root@filesrv1 ~]# service ntpd start
Starting ntpd:                                             [  OK  ]
[root@filesrv1 ~]#
```

Figura 3.4 Sincronización de reloj

- Configurar el inicio del servidor ntp

```
[root@filesrv1 ~]# chkconfig --level 235 ntpd on
[root@filesrv1 ~]# chkconfig  --list ntpd
ntpd            0:off   1:off   2:on    3:on    4:off   5:on    6:off
[root@filesrv1 ~]#
```

Figura 3.5 Configuración de servicio ntpd

3.5.2.2. Resolución de nombres de dominio

Para una correcta resolución de nombres de dominios entre ambos sistemas es un requisito esencial configurar dentro del sistema Linux los DNS lookups del dominio Active Directory. Inconvenientes en la resolución de nombres es una de las principales causas en el fallo de la integración. Para esto es necesario realizar los siguientes paso:

- Editar el archivo de configuración /etc/resolv.conf añadiendo las líneas search y domain con el nombre de dominio FQDN de los servidores DNS

```
# Generated by NetworkManager
domain seei.com
search seei.com
nameserver 192.168.0.100
nameserver 192.168.0.1
```

Figura 3.6 Configuración de DNS

- Anadir en el archivo /etc/hosts la dirección IP con el nombre de dominio FQDN y nombre del servidor.

```
192.168.0.210   filesrv1.seei.com       filesrv1        # Added by NetworkManager
127.0.0.1       localhost.localdomain   localhost
::1     filesrv1.seei.com       filesrv1        localhost6.localdomain6 localhost6
```

Figura 3.7 Resolución de hostname

3.5.2.3. Instalación y configuración de Kerberos.

La instalación del cliente Kerberos krb5-worktstation nos permite asegurar si existe una apropiada autenticación contra el Active Directory del servidor Windows, es un paso muy recomendado para la resolución de problemas e inconvenientes con la autenticación Kerberos.

- Verificar si se encuentra instalado

```
[root@filesrv1 ~]# yum list installed | grep krb5
krb5-libs.i686          1.8.2-3.el6      @anaconda-centos-201106051823.i386/6.0
krb5-workstation.i686   1.8.2-3.el6      @anaconda-centos-201106051823.i386/6.0
pam_krb5.i686           2.3.11-1.el6     @anaconda-centos-201106051823.i386/6.0
```

Figura 3.8 Verificación de Kerberos

- Si no se encuentra instalado, proceder a instalar mediante *yum* o empleando el DVD de instalación de CentOS 6.0, lo cual es más recomendado.

```
[root@filesrv1 ~]# yum -y install krb5-workstation
```

Figura 3.9 Instalación de Kerberos mediante yum

```
[root@filesrv1 ~]# mount /dev/dvd /media
mount: block device /dev/sr0 is write-protected, mounting read-only
[root@filesrv1 ~]# cd /media/Packages/
[root@filesrv1 Packages]# rpm -ivh krb5-workstation-1.8.2-3.el6.i686.rpm
```

Figura 3.10 Instalación de Kerberos mediante paquetes rpm

- Una vez instalado se debe configurar el archivo */etc/krb5.conf* agregando las líneas del servidor Kerberos y el dominio DNS del dominio al cual se desea integrar.

```
[logging]
    default = FILE:/var/log/krb5libs.log
    kdc = FILE:/var/log/krb5kdc.log
    admin_server = FILE:/var/log/kadmind.log

[libdefaults]
 default_realm = SEEI.COM   #Dominio DNS
 dns_lookup_realm = false
 dns_lookup_kdc = false
    ticket_lifetime = 24h
    renew_lifetime = 7d
    forwardable = true

[realms]
    SEEI.COM = {
  kdc = DCSRV1.SEEI.COM              #Servidor Kerberos
  admin_server = DCSRV1.SEEI.COM     #Active Directory server
    }

[domain_realm]
    .demo = SEEI.COM    #Dominio DNS
    demo = SEEI.COM
-- INSERT --                                    22,20         All
```

Figura 3.11 Configuración de kerberos

- Verificar la instalación eliminando cualquier ticket existente, obteniendo uno mediante la cuenta administrador del kdc y listando el ticket.

```
[root@filesrv1 ~]# kdestroy
kdestroy: No credentials cache found while destroying cache
[root@filesrv1 ~]# klist
klist: No credentials cache found (ticket cache FILE:/tmp/krb5cc_0)
[root@filesrv1 ~]# kinit administrador@SEEI.COM
Password for administrador@SEEI.COM:
[root@filesrv1 ~]# klist
Ticket cache: FILE:/tmp/krb5cc_0
Default principal: administrador@SEEI.COM

Valid starting     Expires            Service principal
02/02/14 15:53:06  02/03/14 01:53:09  krbtgt/SEEI.COM@SEEI.COM
        renew until 02/09/14 15:53:06
[root@filesrv1 ~]#
```

Figura 3.12 Verificación de kerberos

Una vez realizada la configuración y comprobado que se puede obtener un ticket de autenticación se pueden emplear los comandos kdestroy, klist y kinit para verificar la funcionalidad de Kerberos en el sistema Linux.

3.5.2.4. Home para los usuarios del dominio

Para crear un home para un usuario del dominio, es necesario emplear el paquete *oddjob-mkhomedir* que permite crear un home cuando el usuario realiza un login en el sistema Linux.

```
[root@filesrv1 ~]# yum -y install oddjob-mkhomedir
```

Figura 3.13 Instalación de oddjob-mkhomedir

3.5.2.5. Instalación y configuración de Samba/Winbind

La siguiente configuración permitirá tener las siguientes ventajas a los sistemas Linux dentro de dominio Active directory o Forest:

- Configuración de la plantilla de usuario (Shell, directorio home)
- SID mapping homogéneo a través de los múltiples sistemas Linux
- Rapidez en ID mapping a través de los sistemas Linux gracias a un algoritmo (idmap_rid)
- No necesita de modificación en los atributos de usuario en el Active Directory
- Autenticación y servicios de compartición de archivos

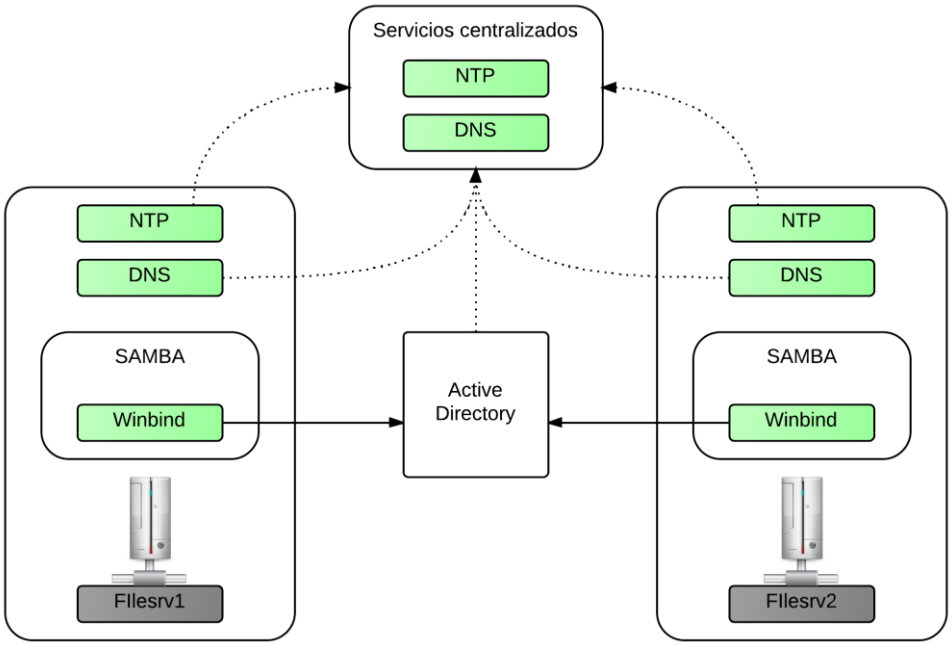

Figura 3.14 Configuración de los sistemas Linux

En la Figura 3.14 se muestra una vista de todos los servicios utilizados y de cómo los sistemas Linux se integran al Dominio. En los siguientes pasos se explicara los pasos y configuraciones que se deben seguir.

Primero se deben instalar los siguientes paquetes via yum o mediante el dvd de instalación de CentOS :

- samba
- samba-client
- samba-common
- samba-winbind
- samba-winbind-clients

```
[root@filesrv1 ~]# yum -y install samba samba-client samba-common samba-winbind
samba-winbind-clients
```

Figura 3.15 Instalación de samba/winbind mediante yum

```
[root@filesrv1 /]# mount /dev/dvd /media/
mount: block device /dev/sr0 is write-protected, mounting read-only
[root@filesrv1 /]# cd /media/Packages/
[root@filesrv1 Packages]# rpm samba-3.5.4-68.el6.i686.rpm samba-client-3.5.4-68.
el6.i686.rpm samba-common-3.5.4-68.el6.i686.rpm samba-winbind-3.5.4-68.el6.i686.
rpm samba-winbind-clients-3.5.4-68.el6.i686.rpm
```

Figura 3.16 Instalación de samba/winbind mediante paquetes rpm

Los parámetros que se emplearan y agregaran al archivo de configuración de samba /etc/samba/smb.conf serán explicados es la siguiente tabla:

Parámetro	Descripción	
imad uid = 100000-199999	Establece el rango de id de usuario para el backend por default (tdb)	
idmap gid = 1000-19999	Establece el rango de id de grupo para el backend por default (tdb)	
idmap config SEEI:backend = rid	Configura el uso del idmap_rid por winbind	
idmap config SEEI:range = 10000-19999	Establece el rango para el idmap_rid	
idmap config SEEI:base_rid = 0	Establece la base del idmap_rid	
winbind enum users = no	Deshabilita la enumeración de usuarios	*Recomendado en ambientes con muchos usuarios
winbind enum groups = no	Deshabilita la enumeración de grupos	

winbind separator = +	Cambia el separador por defecto '\' a '+' para minimizar el scaping del shell, ejemplo : ("DEMO+user" vs. "DEMO\\user")
winbind use default domain = yes	Eliminar la necesidad de especificar el dominio en los comandos
template homedir = /home/%D/%U	Establece el directorio home en /home/SEEI/user

Tabla 3.1 Parámetros de configuración de samba

La manera en que el sistema Linux obtiene el RID del ID de usuario es:

- RID = UNIX_ID + Base_RID - LOW_Range_ID
- UNIX ID = RID – Base_RID + Low_Range_ID

El primer paso que debemos seguir es respaldar la configuración actual de samba y modificar el archivo.

```
[root@filesrv1 ~]# cp -p /etc/samba/smb.conf /etc/samba/smb.conf.back
[root@filesrv1 ~]#
```

Figura 3.17 Respaldo de la configuración de samba

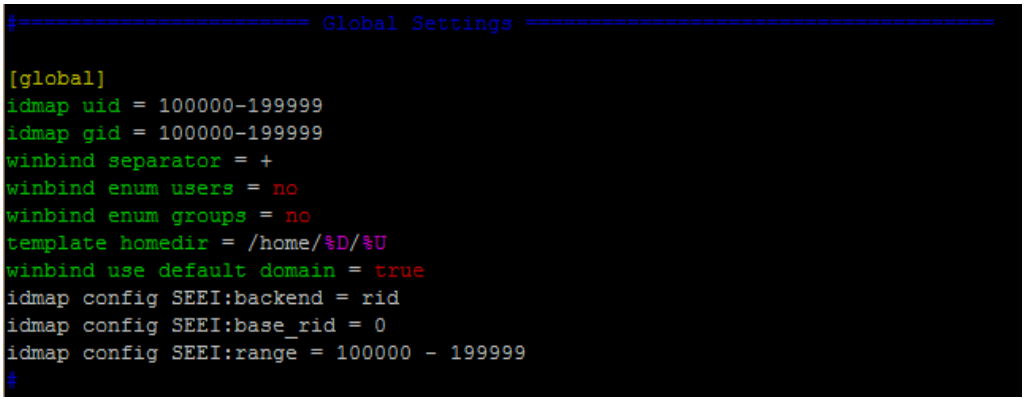

Figura 3.18 Configuración del archivo smb.conf

Una vez modificada la configuración procedemos a realizar la tarea de configurar la autenticación, para esto emplearemos la herramienta system-config-authentication que simplifica la configuración de Samba, Seguridad, kerberos y archivos de autenticación para la integración con el Active Directory. El siguiente comando permite su ejecución:

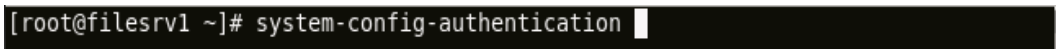

Figura 3.19 Comando de ejecución de la herramienta de autenticación

En el tab Identity & Authentication no dirigimos a User Acconut Database y seleccionamos **Winbind.**

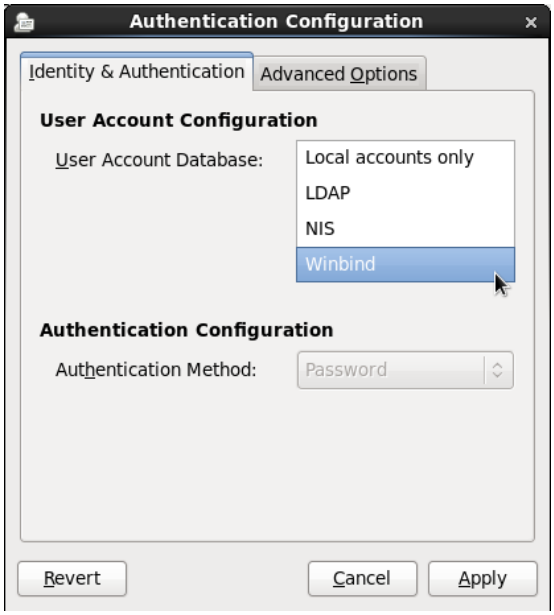

Figura 3.20 Herramienta de autenticación tab 1

Una vez seleccionada la opción se mostraran nuevos campos de configuración:

- **Winbind Domain:** Es el domino Windows Active Directory
- **Security Model:** Modo de operación de Samba, el cual permite seleccionar varias opciones
    - ads: Este modo permite a Samba actuar como un miembro del dominio DNS al cual se desea Integrar.
- **Winbind ADS realm:** una vez seleccionado el Security Model en ads, debemos espeficicar el dominio DNS del cual será miembro.

- **Winbind Domain Controllers:** Especifica con que controlador de dominio será usado Winbind.
- **Template Shell:** El demonio Winbind usa este valor para especificar el Login Shell de los usuarios del dominio
- **Allow Offline login:** La información de la autenticación será almacenada en cache.

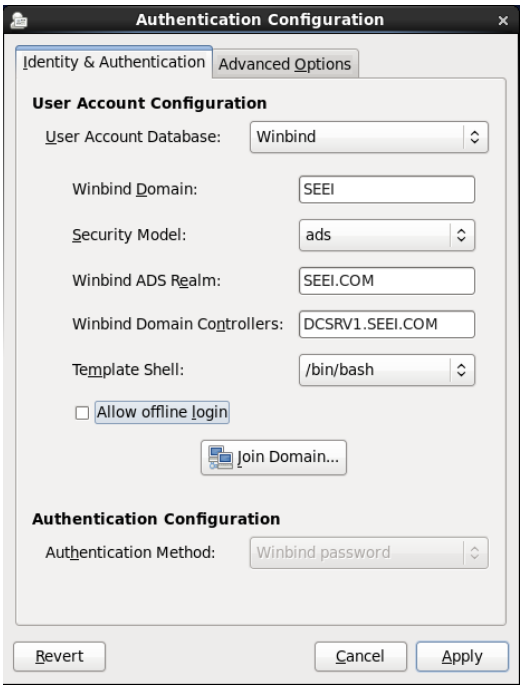

Figura 3.21 Herramienta de autenticación tab 2

En el tab de Advanced Options seleccionamos la opción de crear directorio Home al primer login.

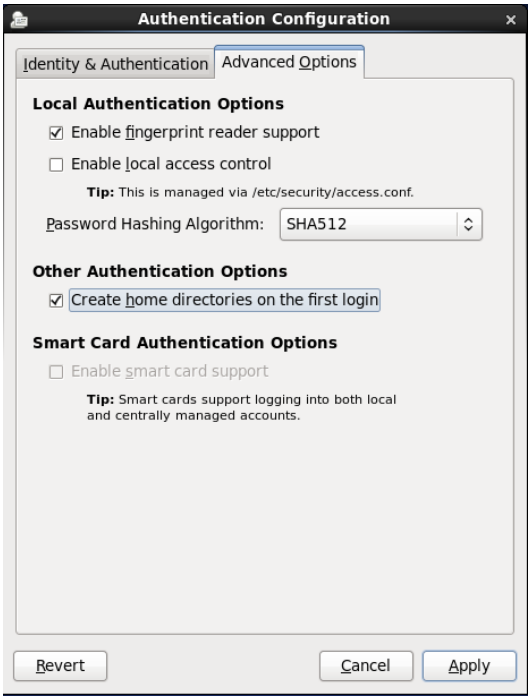

Figura 3.22 Herramienta de autenticación tab de advance options

Una vez configurado esto, volvemos al tab de Identity & Authentication, damos click en join domain, aparecerá una alerta que nos pedirá guardar la configuración, nos pedirá el usuario y contraseña del administrador del DC.

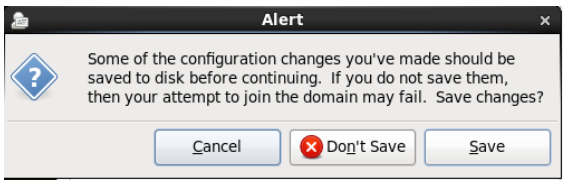

Figura 3.23 Herramienta de autenticación mensaje de alerta

Figura 3.24 Herramienta de autenticación ventana de integración

Después de ingresado el usuario y password correcto veremos en la terminal desplegarse la siguiente información que nos indicara una exitosa integración.

```
[root@filesrv1 ~]# system-config-authentication
Starting Winbind services:                                 [  OK  ]
Starting oddjobd:                                          [  OK  ]
[/usr/bin/net join -w SEEI -S DCSRV1.SEEI.COM -U Administrador]
Enter Administrador's password:<...>

Using short domain name -- SEEI
Joined 'FILESRV1' to realm 'seei.com'
```

Figura 3.25 Integración exitosa

Mediante los comandos net ads testjoin y net ads info podemos obtener información de la integración con el dominio Active Directory.

```
[root@filesrv1 ~]# net ads testjoin
Join is OK
[root@filesrv1 ~]# net ads info
LDAP server: 192.168.0.100
LDAP server name: dcsrv1.seei.com
Realm: SEEI.COM
Bind Path: dc=SEEI,dc=COM
LDAP port: 389
Server time: Mon, 03 Feb 2014 01:36:18 ECT
KDC server: 192.168.0.100
Server time offset: 2
[root@filesrv1 ~]#
```

Figura 3.26 Prueba de integración

Para obtener información de los grupos y usuarios del dominio Active Directory debemos utilizar los comando wbinfo --domain-gropus y wbinfo --domain-user.

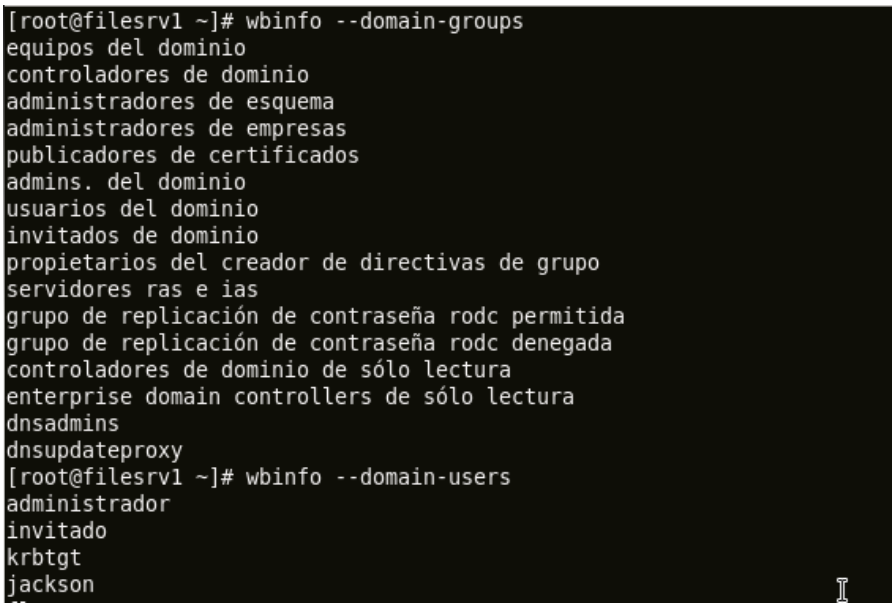

Figura 3.27 Prueba de usuarios y grupos

Si queremos mantener una lista local actualizada de los grupos y usuarios debemos realizar la acción de join domain con la herramienta system-config-authentication

Para verificar la autenticación del usuario realizaremos una conexión ssh con un usuario del dominio Active Directory con el servidor Linux configurado como destino, después del obtener el acceso ejecutaremos una serie de comando para obtener información.

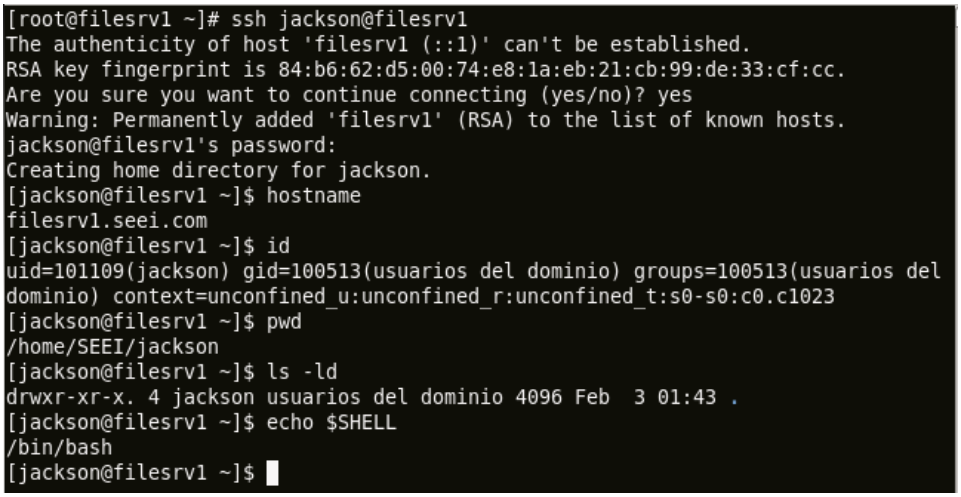

Figura 3.28 Prueba de autenticación

3.6. Implementación de operatividad vía web

El objetivo principal es poder implementar una herramienta web que facilite todo el proceso de integración mediante petición de parámetros de pre configuración y datos sobre el Dominio Windows Active directory.

Para obtener este producto final se emplearon lenguajes de programación CSS, HTML, javaScript y PHP este último permite una gran interacción con el sistema en el que se ejecuta la aplicación mediante la ejecución de sentencias de ejecución y scripts, la extensión ssh2 que permite emplear la libssh2 permite interactuar con otros sistemas mediante una conexión SSH entre el servidor en donde se encuentra la aplicación y el equipo cliente. De esta manera es posible configurar varios sistemas Linux sin la necesidad de instalar la

aplicación en cada sistema Linux que se desee integrar al dominio Active Directory.

3.6.1. Preparación del entorno

Es necesario que el servidor Linux donde se desplegara la aplicación se encuentre habilitado y configurado como un servidor web con la capacidad de ejecutar aplicaciones desarrolladas en PHP.

La extensión ssh2 se deberá instalar mediante los siguientes pasos:

- Comprobar si la librería libssh2 se encuentra instalada, caso contrario se deberá proceder a instalar mediante el DVD de instalación de CentOS.

```
[root@filesrv1 ~]# rpm -q libssh2
libssh2-1.2.2-7.el6.i686
```

Figura 3.29 Verificación de librería libssh2

```
[root@filesrv1 ~]# cd /media/CentOS_6.0_Final/Packages/
[root@filesrv1 Packages]# rpm -ivh libssh2-1.2.2-7.el6.i686.rpm
```

Figura 3.30 Instalación de librería mediante paquete rpm

- Comprobar si se encuentra instalado el paquete de desarrollo de PHP php-devel, caso contrario se deberá proceder a instalar mediante el DVD de instalación de CentOS.

```
[root@filesrv1 ~]# rpm -q php-devel
php-devel-5.3.2-6.el6.i686
```

Figura 3.31 Verificación de php-devel

```
[root@filesrv1 ~]# cd /media/CentOS_6.0_Final/Packages/
[root@filesrv1 Packages]# rpm -ivh php-devel-5.3.2-6.el6.i686.rpm
```

Figura 3.32 Instalación de paquete php-devel mediante paquete rpm

3.6.2. Desarrollo de la herramienta

La herramienta contendrá el número de interfaces que se plantearon en el Diseño web y tendrá los elementos mencionados en el diseño de cada interfaz. Se expondrá el código que se empleó para ejecutar los procesos que se ejecutan en cada interfaz y su funcionamiento.

3.6.2.1. Interfaz de Login

El archivo index.php es el primero en llamarse y contendrá la interfaz de login, está a su vez contendrá los elementos previamente hablados en su diseño.

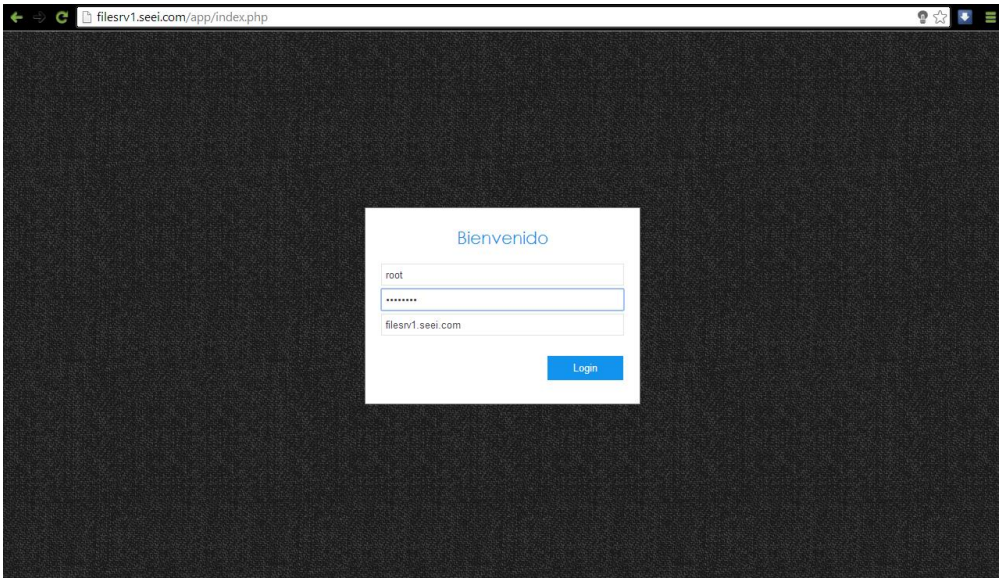

Figura 3.33 Pantalla de Login

Si el usuario se encontraba previamente con una sesión iniciada se enviara directamente a la interfaz de Host caso contrario deberá ingresar la información del formulario.

Cuando el usuario ingresa todos sus datos y da click en el botón Login se llama a la función *valida_usuario.php* la cual comprueba si es un usuario del sistema Linux y del grupo root; para redijirlo a la interfaz del Host, caso contrario enviara un mensaje de error

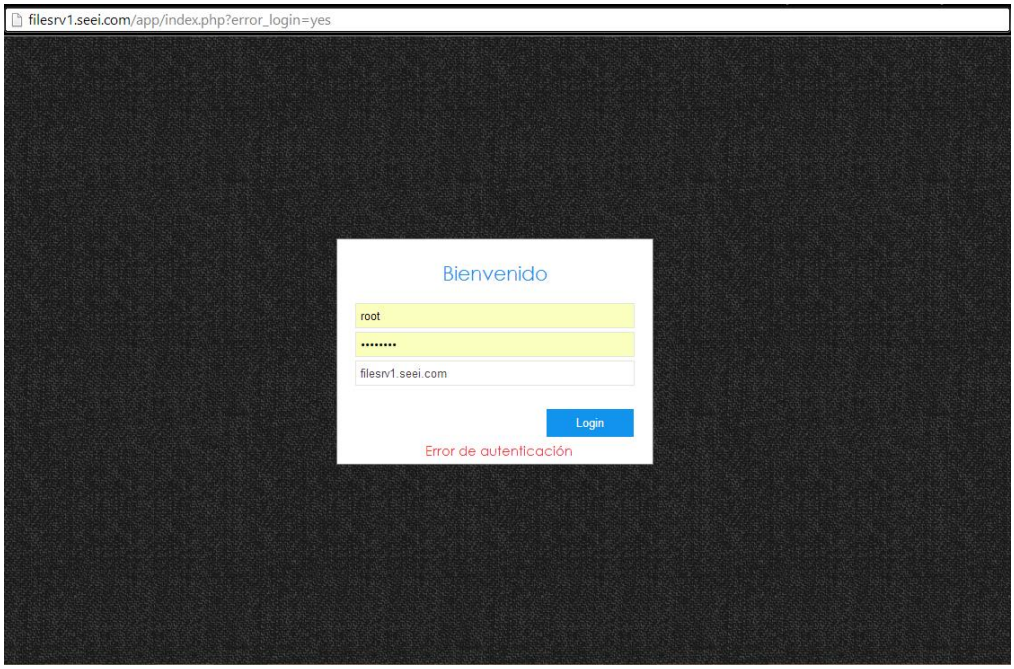

Figura 3.34 Error de Autenticación

```php
<?php
include 'servers.php';
include 'funciones_db.php';
if($_POST['servidor']!="" && $_POST['admin']!="" && $_POST['password_usuario']!="" ){
    $servidor=$_POST['servidor'];
    $connection = ssh2_connect($servidor, 22);
    $usuario = $_POST['admin'];
    $password = $_POST['password_usuario'];
    if (ssh2_auth_password($connection, $usuario, $password)) {
        session_start();
        $_SESSION['autenticado'] = TRUE;
        $_SESSION['usuario'] = $usuario;
        $_SESSION['password'] = $password;
        $_SESSION['servidor'] = $servidor;
        $_SESSION['dominio']=FALSE;
        crear_db('Integracion.db');
        if(data_host()){
            host_db('Integracion.db');
        }
        paquetes();
        header('Location: ../Host.php');
    } else {
        header('Location: ../index.php?error_login=yes');
    }
}else{
    header('Location: ../index.php?error_login=yes');
}
?>
```

Figura 3.35 Función validar_usuario.php

En la Figura. 3.35 se muestra el código de la función, esta emplea la extensión ssh2 para iniciar una sesión

SSH contra el equipo con el cual desea iniciar sesión. Si la autenticación es exitosa se ejecutan las funciones:

- **crear_db** que crea una base de datos basada en SQLite en el cual se almacenara información de los sistemas Linux que sean integrados al dominio Active Directory
- **data_host** que obtiene información sobre el grupo al que pertenece el usuario, la dirección IP del equipo, el Nombre de dominio del equipo, la arquitectura del sistema Linux y si se encuentra enlazado a un dominio Active Directory.
- **host_db** ingresa la información obtenida del sistema Linux a la base creada
- **paquetes** obtiene información sobre los paquetes necesarios para la integración, si el sistema Linux no posee todos los paquetes será enviado directamente a la interfaz de Información

Si el usuario no pertenece al grupo root será enviado a la interfaz de Información y solo podrá ingresar a esa interfaz y a la interfaz de Servidores.

3.6.2.2. Interfaz de Host

Es la interfaz principal de la herramienta y sirve para la pre configuración del sistema, en esta primera interfaz se muestra información básica del sistema y de la herramienta ubicada en la cabecera, al usuario.

Figura 3.36 Cabecera de la interfaz

Si en navegador no tiene activado la ejecución de javaScript se mostrar la siguiente advertencia.

Figura 3.37 Advertencia de uso de javaScript

Esta cabecera aparecerá en todas las páginas y en la parte superior derecha se mostrar el link para cerrar la sesión del usuario.

En la parte central se encuentran los formularios de configuración y ventanas de información que se despliegan al momento de acercar el puntero a uno de

los formularios, explicando de una manera corta y sencilla la función de cada campo.

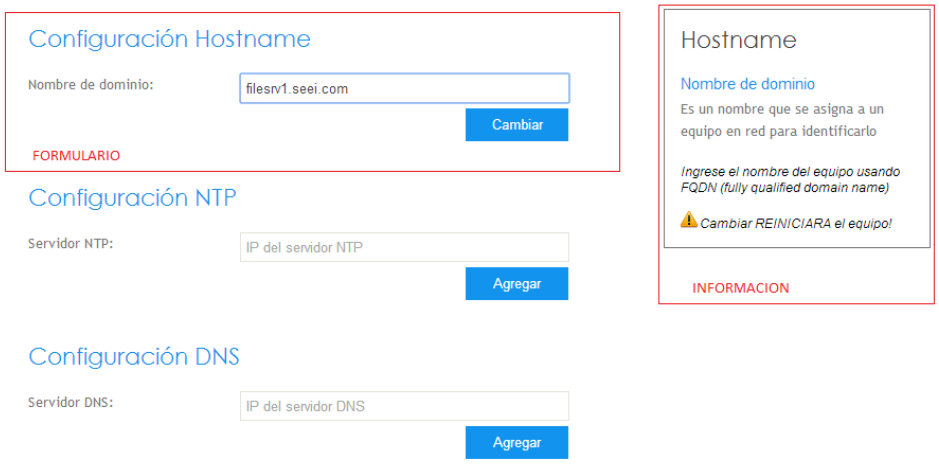

Figura 3.38 Distribución de loa formularios en la interfaz Host

Los formularios funcionan de la siguiente manera:

- Todos los formularios validan que no se envíen datos nulos o en blanco y unos emplean el archivo validad.php con las funciones validar_nombre y validar_ip4 para realizar una validación extra.

```php
<?php
    function validar_nombre($nombre){
        $permitidos='abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789-_.';
        for ($i=0; $i<strlen($nombre); $i++){
            if (strpos($permitidos, substr($nombre,$i,1))===false){
                return false;
            }
        }
        return true;
    }

    function validar_ip4($ip){
        if(filter_var($ip, FILTER_VALIDATE_IP)){
            return true;
        }else{
            return false;
        }
    }
?>
```

Figura 3.39 código del archivo validar. php

- Configuración Hostname: llama a la función hostname.php la cual realiza la validación del nuevo nombre de dominio mediante la función validar_nombre que verifica el formato FQDN, el cambio de nombre de dominio, la actualización los datos del equipo en la base, el reinicio el sistema y el cierre de sesión del usuario.

```php
<?php
    include 'coneccion.php';
    include 'validar.php';
    if($_POST['nombre']!=""){
        if(validar_nombre($_POST['nombre'])){
            session_start();
            $host=explode(".",$_POST['nombre']);
            ejecutar('sed -i".old" \'/HOSTNAME/d\' /etc/sysconfig/network');
            ejecutar('echo \'HOSTNAME='.$_POST['nombre'].'\' >> /etc/sysconfig/network ');
            $var=ejecutar('grep '.$_POST['nombre'].' /etc/sysconfig/network');
            if($var['out']!=""){
                cambiar_host('Integracion_db');
                ejecutar('init 6');
                session_destroy();
                header('location: ../index.php');
            }else{
                header('location: ../Host.php?error=host1');
            }
        }else{
            header('location: ../Host.php?error=host0');
        }
    }else{
        header('location: ../Host.php?error=host0');
    }
?>
```

Figura 3.40 Código de la función hostname.php

- Configuración NTP: llama a la función ntp.php que realiza la configuración de sincronización de reloj.

```php
<?php
include 'coneccion.php';
$server=$_POST['ipserver'];
if($server!=""){
    $var=ejecutar('service ntpd stop | grep -E "OK|FAILED"');
    if ($var['out']!="") {
        $var=ejecutar('ntpdate '.$server.' | grep \'no server\'');
        if($var['error']=="") {
            $var=ejecutar('grep -w "server '.$server.'" /etc/ntp.conf');
            if($var['out']==""){
                ejecutar('sed -i".old" \'$a server '.$server.'\' /etc/ntp.conf');
                $var=ejecutar('grep   "server '.$server.'" /etc/ntp.conf');
                if($var['out']!=""){
                    $var=ejecutar('service ntpd start | grep -E "OK|Starting"');
                    if ($var['out']!=""){
                        header ('Location: ../Host.php?error=ntp_yes');
                    }else{
                        header ('Location: ../Host.php?error=ntp4');
                    }
                }else {
                    header ('Location: ../Host.php?error=ntp3');
                }
            }else{
                header ('Location: ../Host.php?error=ntp_yes');
            }
        }else {
            header ('Location: ../Host.php?error=ntp2');
        }
    }else {
        header ('Location: ../Host.php?error=ntp1');
    }
}else{
    header ('Location: ../Host.php?error=ntp0');
}
?>
```

Figura 3.41 Código de la función ntp.php

- Configuración DNS: llama a la función dns.php que validad mediante la función validar_ip4 si el dato ingresado es una dirección IPv4 validad y realiza la configuración de resolución de nombres de domino.

```php
<?php
    include 'coneccion.php';
    include 'validar.php';
    if($_POST['dnsserver']!=""){
        if(validar_ip4($server)){
            ejecutar('sed -i".old" \'$a nameserver '.$_POST['dnsserver'].'\' /etc/resolv.conf');
            $var=ejecutar('grep -w '.$_POST['dnsserver'].' /etc/resolv.conf');
            if($var['out']){
                header ('Location: ../Host.php');
            }else{
                header ('Location: ../Host.php?error=dns1');
            }
        }else{
            header ('Location: ../Host.php?error=dns0');
        }
    }else{
        header ('Location: ../Host.php?error=dns0');
    }
?>
```

Figura 3.42 Código de la función dns.php

Después de ejecutada la configuración se mostraran los siguientes mensajes de error o éxito en la ejecución.

Una vez realizada la sincronización y agracacion del servidor NTP al sistema Linux, el mensaje de éxito será como se muestra en la Fig. 3.43

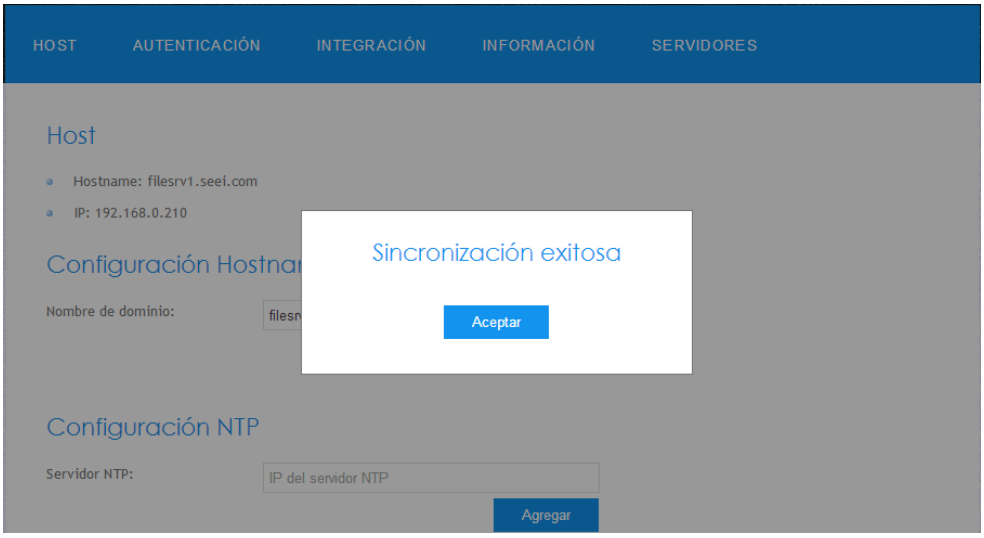

Figura 3.43 Mensaje de éxito de las configuraciones NTP

El La validación de los datos que ingresa en los campos requeridos permite evitar una mala configuración por parte del ususario, el mensaje de error se encuentra en la Fig. 3.44.

Figura 3.44 Ingreso de valores NTP y DNS inválidos

Si el servicio ntpd no puede ser detenido por la herramienta se mostrar el mensaje error de la Fig. 3.45.

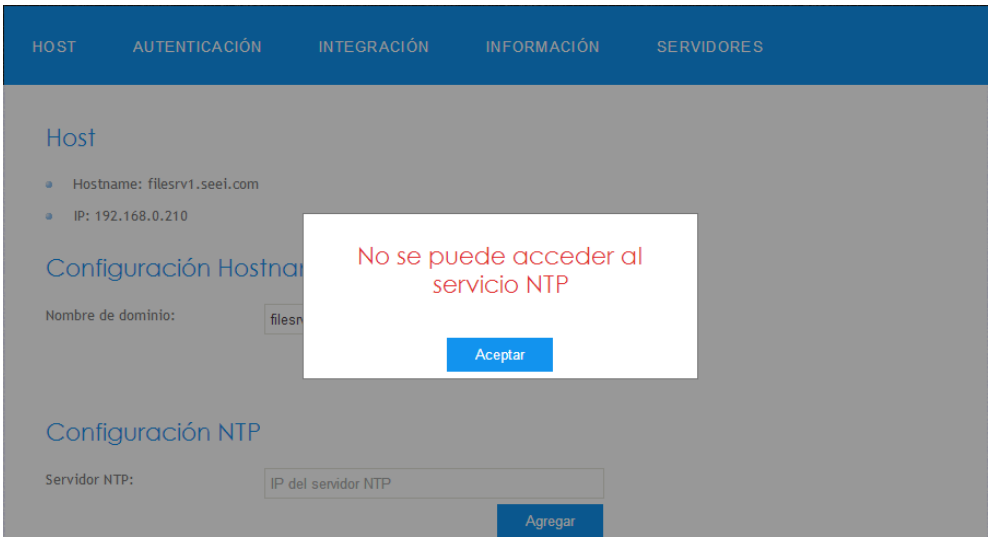

Figura 3.45 error en la detención del servicio ntpd

Una sincronizacion fallifa en el proceso de configuración de NTP, muestra el mensaje de la Fig. 4.46

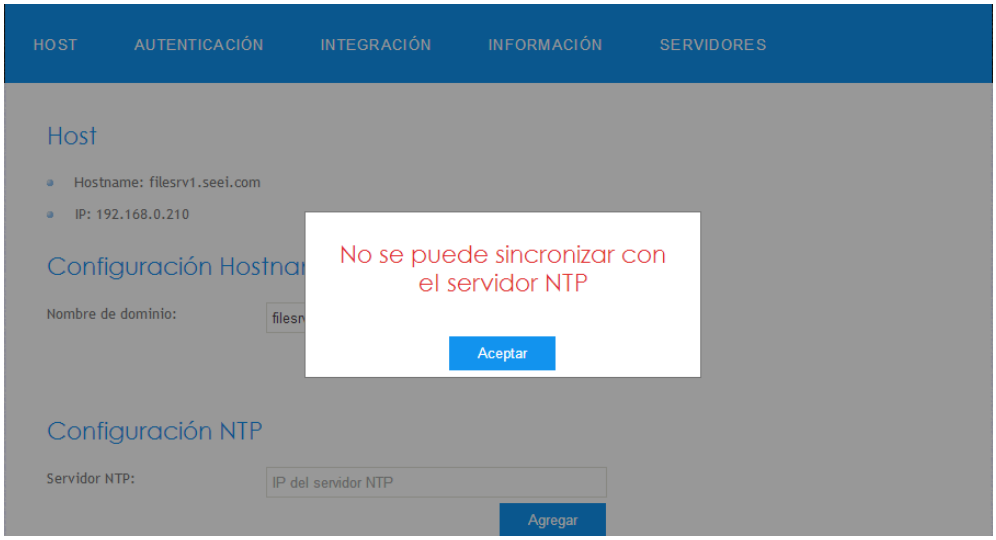

Figura 3.46 Error al sincronizar con el servidor NTP

Si no se puede agregar el servidor NTP al archivo de configuración, se mostrara el mensaje de error Fig. 3.47

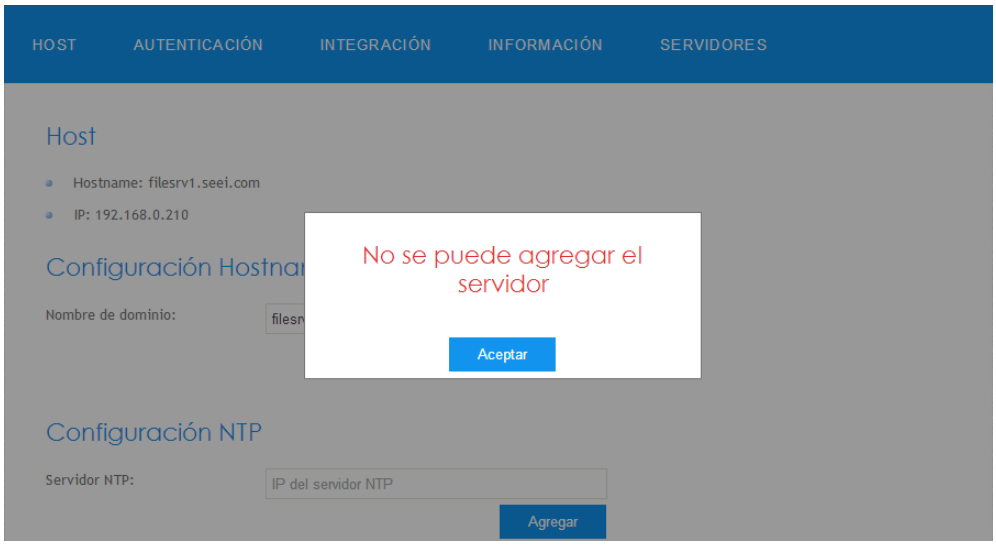

Figura 3.47 Error al guardar el servidor NTP

Cuando ocurre un fallo en el inicio del servicio ntpd durante el proceso de configuacion NTP, muestra el mensaje de error de la Fig. 3.48

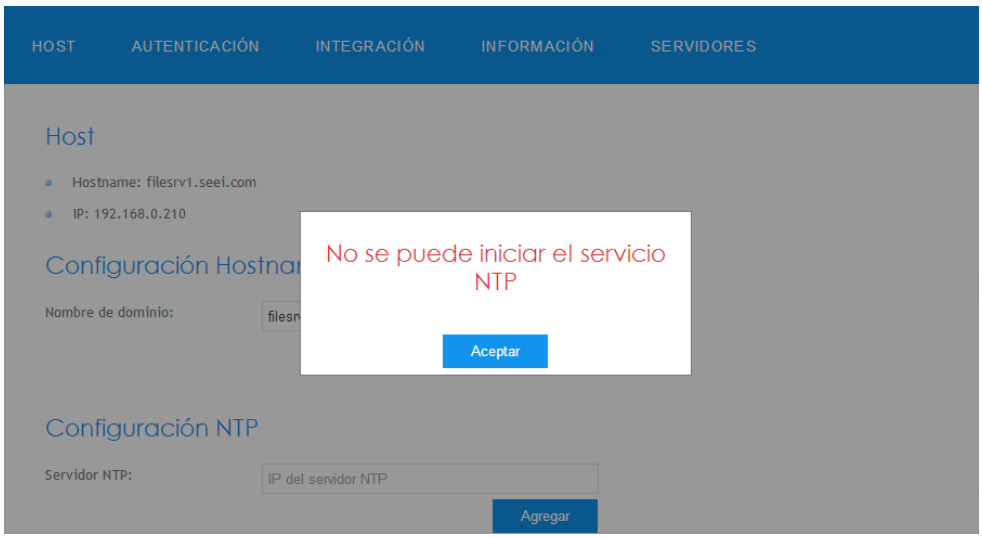

Figura 3.48 Error al iniciar el servicio ntpd

El no poder agregar el servidor DNS al archivo de configuración, genera el mensaje de error de la Fig. 3.49

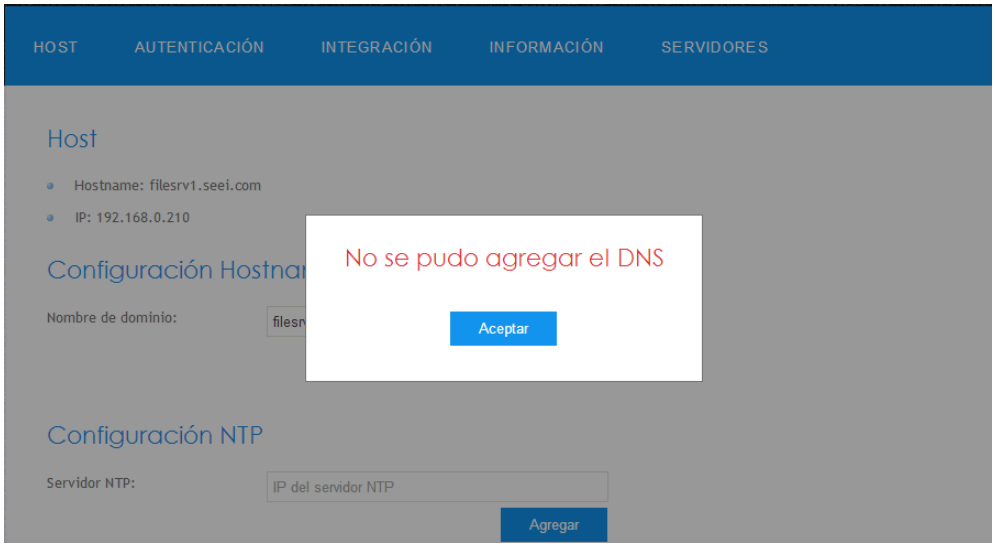

Figura 3.49 Error al modificar el archivo /etc/resolv.conf

En la parte inferior se mostrara la información actual y recientemente agregada de los servidores NTP y DNS, dichos servidores mostrados podrán ser eliminados mediante el link eliminar. En la tabla de servidores NTP se muestra el link de sincronizar que permita la sincronización de reloj con el servidor elegido.

Figura 3.50 Información de la interfaz de Host

La información mostrada en las tablas es llenada gracias a las funciones servers_ntp y servers_dns que buscan

en los archivos de configuración del sistema Linux los servidores NTP y DNS existentes. La información obtenida es agregada a la base.

```
function servers_ntp(){
    $comando='grep ^server /etc/ntp.conf | awk \'{ print $2 }\'';
    $var=ejecutar($comando);
    $servers = explode("\n", $var['out']);
    return $servers;
}

function servers_dns(){
    $comando='grep ^nameserver /etc/resolv.conf | awk \'{ print $2 }\'';
    $var=ejecutar($comando);
    $servers = explode("\n", $var['out']);
    return $servers;
}
```

Figura 3.51 Funciones servers_ntp y servers_dns

El link eliminar de la tabla servidores NTP llama a la función eliminar_ntp, que quita el servidor del archivo /etc/ntp.conf y de la base, si el servidor no puede ser eliminado muestra un mensaje de error.

```
1  <?php
2      include 'coneccion.php';
3      include 'funciones_db.php';
4      ejecutar('sed -i".old" \'s/\<server '.$_GET['server'].'\>//g\' /etc/ntp.conf');
5      $var=ejecutar('grep -w '.$_GET['server'].' /etc/ntp.conf');
6      if($var['out']==""){
7          ntp_remove_db('Integracion.db',$_GET['server']);
8          header ('Location: ../Host.php');
9      }else{
10         header ('Location: ../Host.php?error=ntp5');
11     }
12 ?>
```

Figura 3.52 Función eliminar_ntp

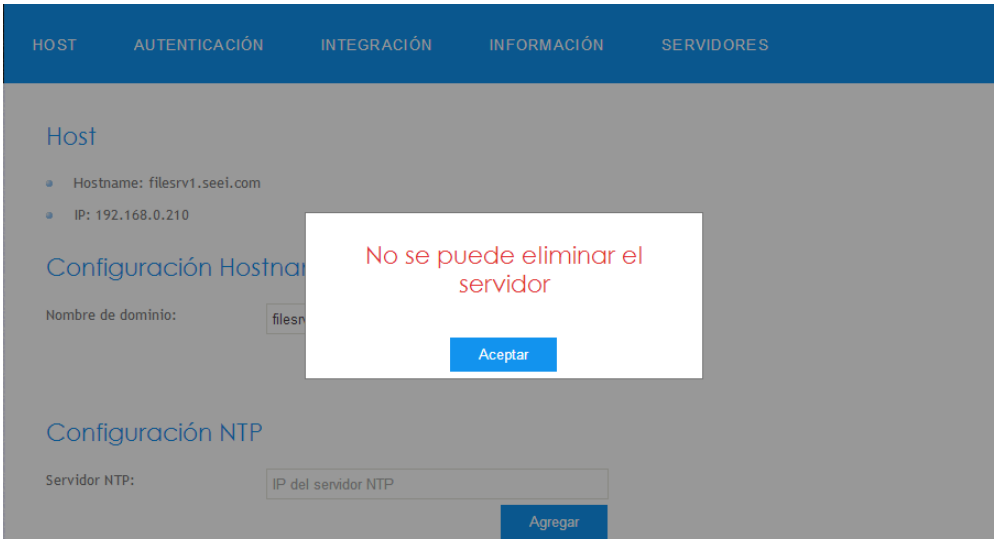

Figura 3.53 Mensaje de error de la función eliminar_ntp

El link sincronizar ejecuta la función sincronizar, que actualiza el reloj con el servidor elegido, de suceder algún error se enviara un mensaje de error que se muestra en la Figura 3.53.

```php
<?php
    include 'coneccion.php';
    $var=ejecutar('service ntpd stop | grep -E "OK|FAILED"');
    if ($var['out']!=""){
    $var=ejecutar('ntpdate '.$_GET['server'].' | grep "no server"');
        if ($var['error']=="") {
            $var=ejecutar('service ntpd start | grep -E "OK|Starting"');
            if ($var['out']!=""){
              header ('Location: ../Host.php?error=ntp_yes');
            }else{
              header ('Location: ../Host.php?error=ntp4');
            }
        }else{
            header ('Location: ../Host.php?error=ntp2');
        }
    }else{
        header ('Location: ../Host.php?error=ntp1');
    }
?>
```

Figura 3.54 Función sincronizar

El link eliminar de la tabla servidores DNS quita el servidor del archivo de configuración /etc/resolv.conf y de la base, de no poder eliminarse se envía un mensaje de error.

```php
<?php
    include 'coneccion.php';
    include 'funciones_db.php';
    ejecutar("sed -i\".old\" 's/\<nameserver ".$_GET['dnsserver']."\>//g' /etc/resolv.conf");
    $var=ejecutar('grep -w '.$_GET['dnsserver'].' /etc/resolv.conf');
    if($var['out']==""){
      dns_remove_db('Integracion.db',$_GET['dnsserver']);
      header ('Location: ../Host.php');
    }else{
      header ('Location: ../Host.php?error=dns2');
    }
?>
```

Figura 3.55 Función eliminar_dns

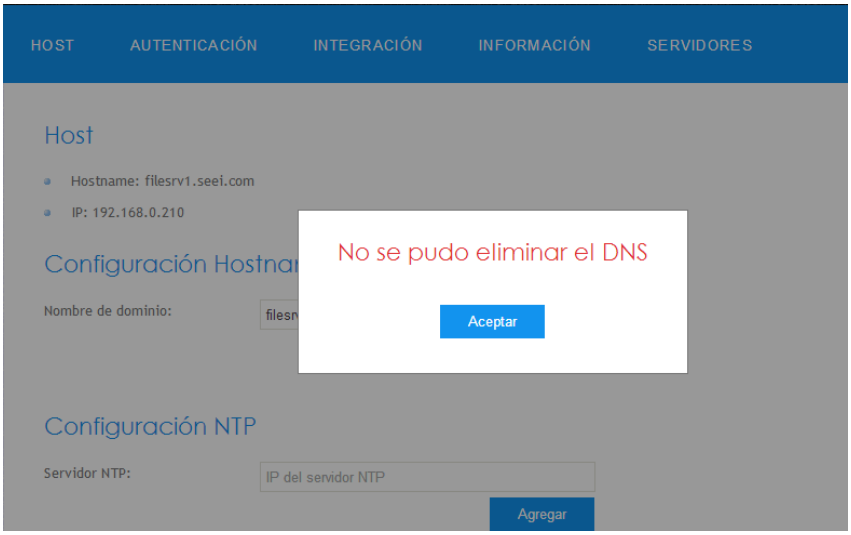

Figura 3.56 Mensaje de error de la función eliminar_dns

3.6.2.3. Módulo de Autenticación

En este módulo se mostrara información y se realizara la configuración de Kerberos, para esto se mostrara un formulario en el cual el usuario deberá ingresas los datos

de dominio y controlador de dominio encargado de la autenticación.

Figura 3.57 Pantalla de autenticación

En la tabla que muestra la información actual del la configuración se encuentran dos enlaces:

- **reset:** permite volver a la configuración por defecto del archivo /etc/krb5.conf.
- **editar:** permite editar la configuración actual del archivo /etc/krb5.conf.

La función encargada de realizar la configuración se llama Kerberos.php la cual valida los datos y modifica el archivo /etc/krb5.conf y el /etc/resolv.conf, agregando los datos ingresados por el usuario en el formulario de la manera correspondiente a su configuración.

Si existe algún error en el proceso de configuración se desplegaran los siguientes mensajes.

El mensaje de error de la Fig. 3.58 indica que se ingreso un dominio y un controlador de dominio sin formato FQDN.

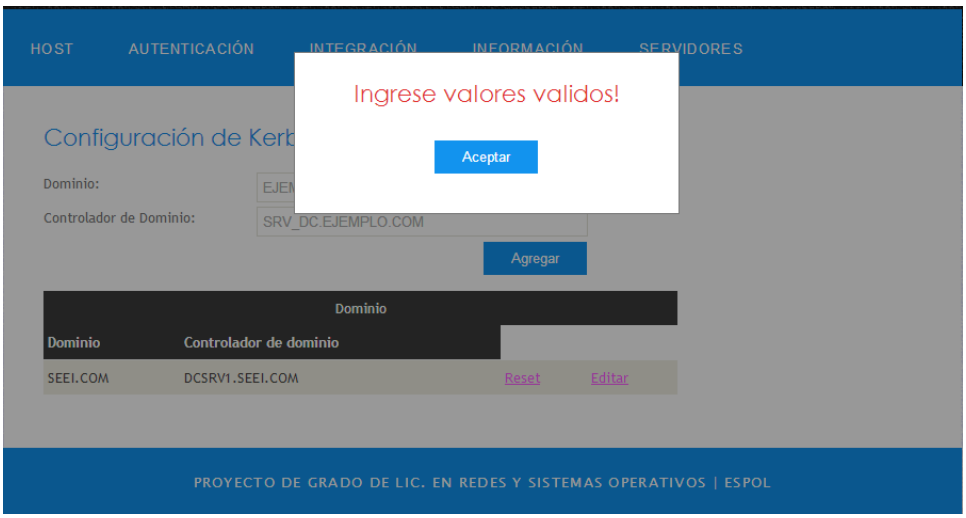

Figura 3.58 Error por ingreso de datos inválidos

Si no es posible editar el archivo de configuración se mostrara el mensaje de error de la Fig. 3.59.

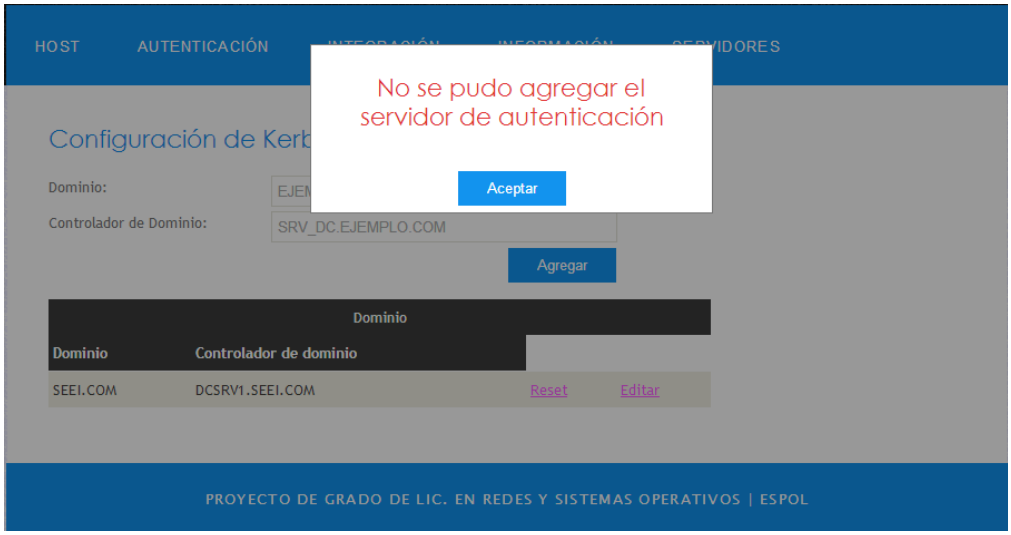

Figura 3.59 Error al modificar el archivo /etc/krb5.conf

El ultimo paso del proceso de configuración es agregar a la configuración DNS el dominio DNS, si no es posible editarlo mostrara el mensaje de error de la Fig. 3.60.

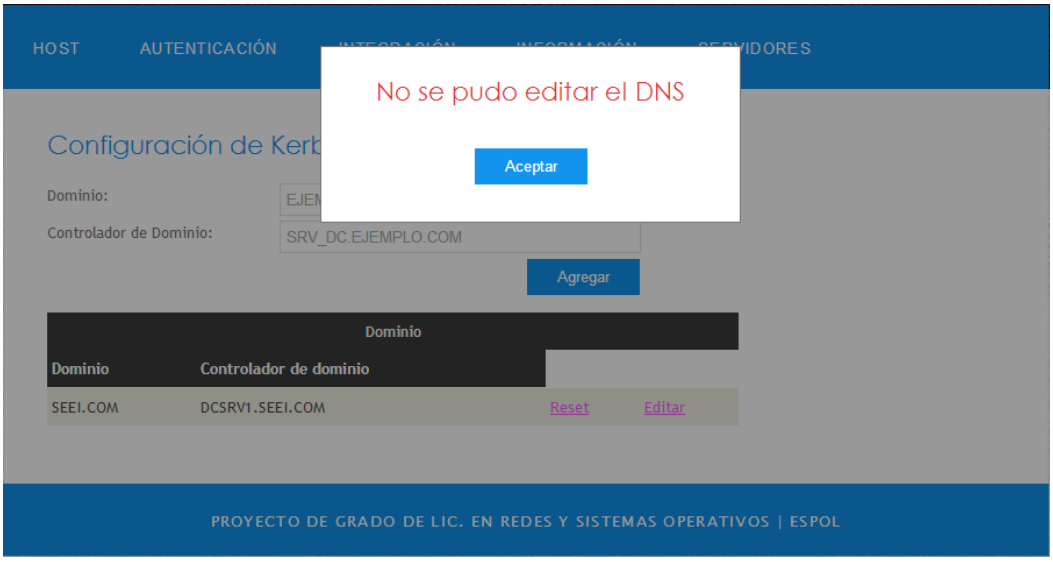

Figura 3.60 Error al editar el archivo /etc/resolv.conf

Si la configuración resulta exitosa se enviara al usuario directamente al módulo de Integración y se mostrara un mensaje de éxito.

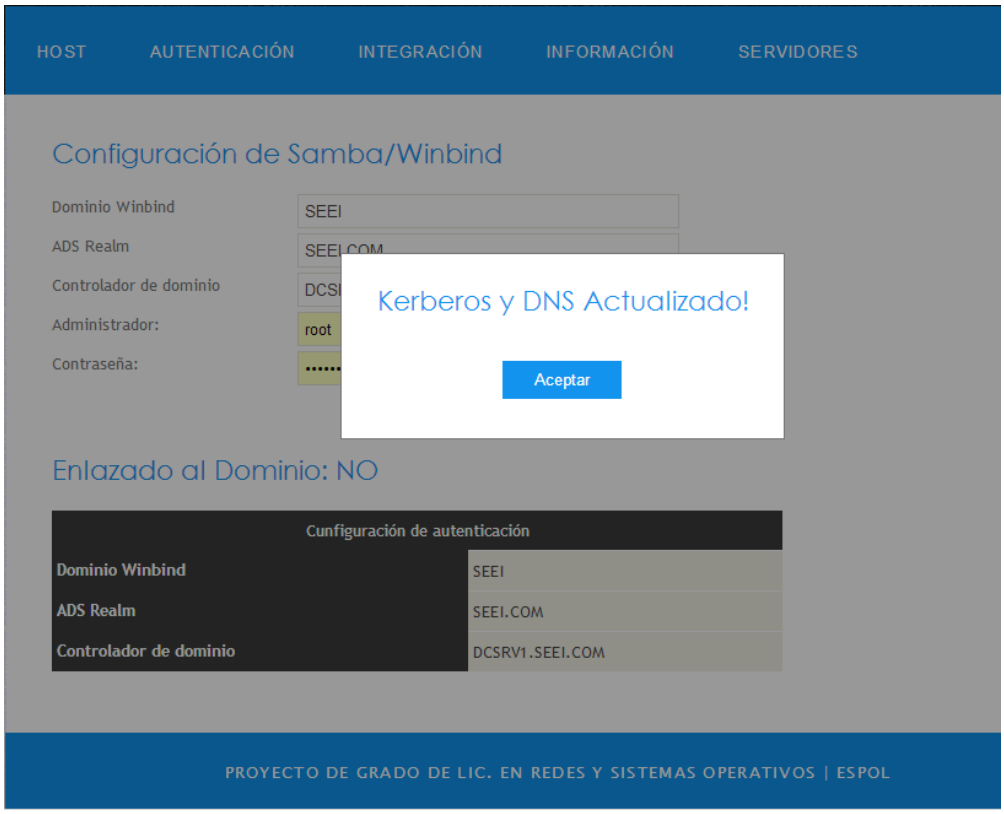

Figura 3.61 Configuración de Kerberos exitosa

3.6.2.4. Módulo de Integración

Dentro del módulo de integración se realizara la configuración de samba para la integración al dominio, permitiendo a los usuarios de este tener acceso s loas recursos del sistema. Si el usuario realizo la configuración en el módulo de autenticación, se

mostraran los valores previamente ingresados en dicho modulo, en sus campos correspondientes dentro de este módulo como una forma de ayuda para el usuario.

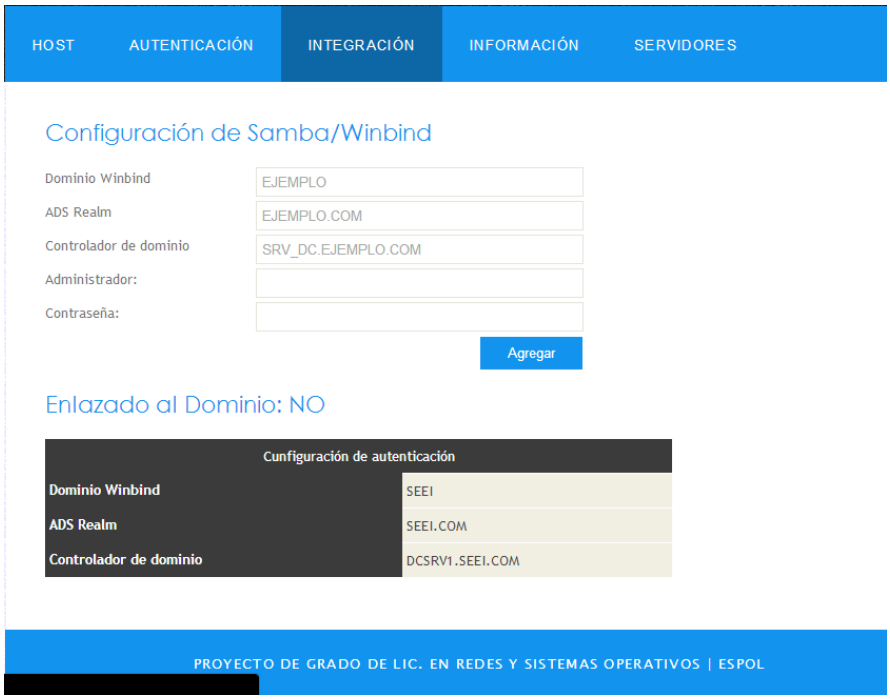

Figura 3.62 Pantalla de integración

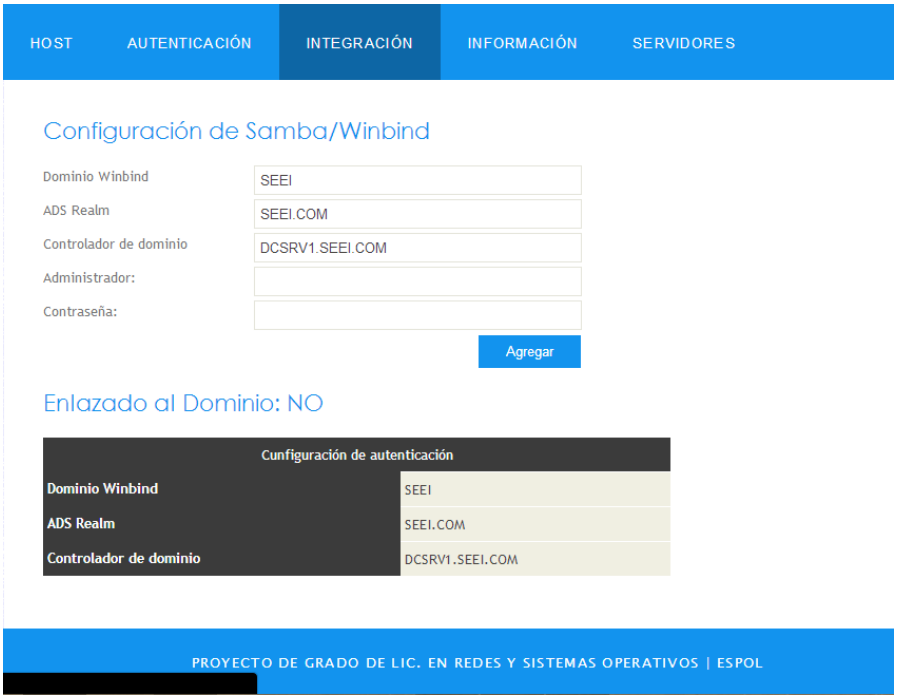

Figura 3.63 Datos del módulo de autenticación.

Dentro del este módulo se encontrara el formulario de configuración, datos sobre el enlace existente y si se encuentra enlazado actualmente o no al dominio.

Los parámetros de configuración que son necesarios son los siguientes:

- Dominio Winbind: es el dominio del cual será parte
- ADS realm: es el dominio DNS.
- Controlador de domino: es el controlador de dominio al cual se integrara

- Administrador y contraseña: Usuario administrador del controlador de dominio

Una vez ingresados los datos correctos damos click en agregar y se llamara a la función authconfig.php que es la encargada de realizar la configuración en el archivo smb.conf y de ejecutar una versión en CLI de la herramienta system-config-authentication.

Si durante el proceso de configuración sucede algún error se mostraran los siguientes mensajes.

Siempre se validan los datos que ingresa el usuario en todos los formularios, el mensaje de error en caso de ser datos no validos, se muestra en la Fig. 3.64

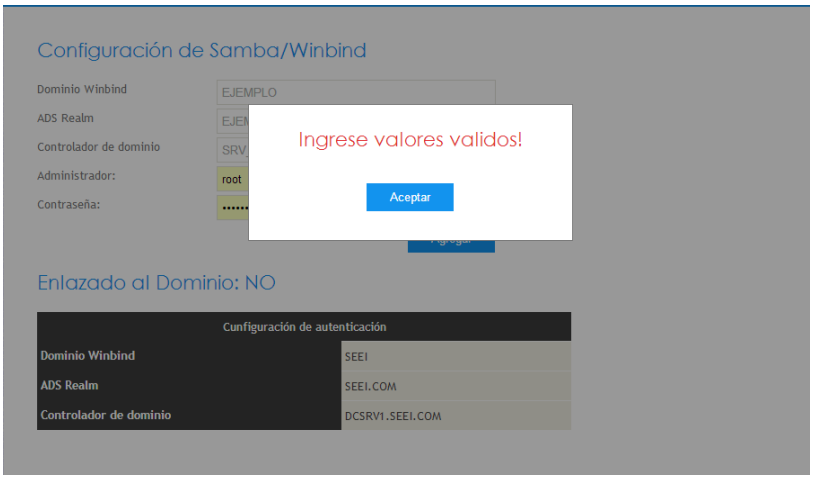

Figura 3.64 Error por valores no validos

Si la integración al dominio no resulta exitosa aparecerá el mensaje de la Fig. 3.65.

Figura 3.65 Error al integrarse al dominio

Si anteriormente se encontraba enlazado a un domino y se enlazaba a uno nuevo el mensaje de error será el siguiente.

Figura 3.66 Error al enlazarse a un nuevo dominio

SI la configuración resulta exitosa se mostrara el siguiente mensaje.

Figura 3.67 Enlace al dominio conexito.

3.6.2.5. Módulo de información

Dentro de este módulo se mostrara información sobre los principales paquetes que son necesarios para la integración al dominio además se podrá monitorear el acceso a los recursos compartidos por el servidor.

Figura 3.68 Pantalla de información.

Si un paquete no se encuentra instalado se mostrara un link que permitirá la instalación del paquete, tanto como para una arquitectura de 32 o 64 bits. Si el paquete no pudo ser instalado se mostrara un mensaje de error.

Figura 3.69 Instalar paquetes

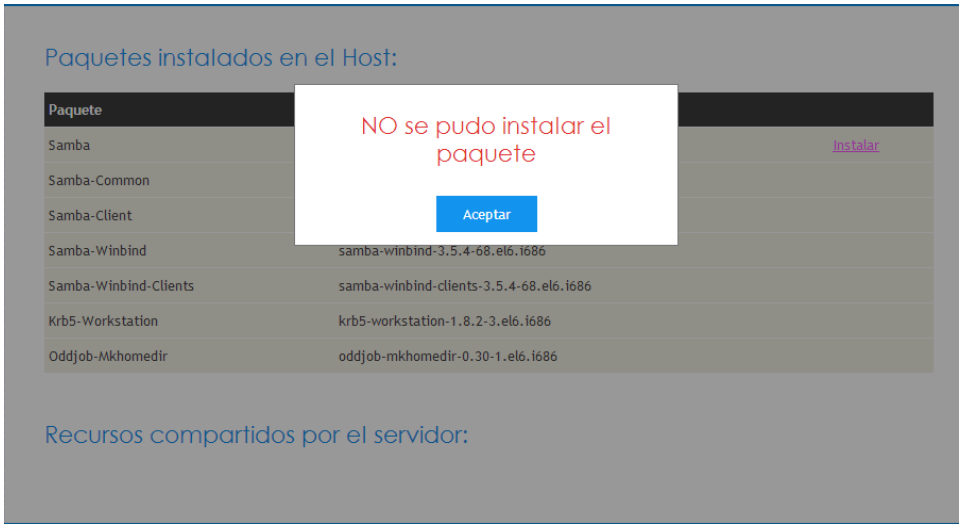

Figura 3.70 Error de instalación.

El acceso a los recursos se mostrara mediante una tabla de información que permitirá ver un detalle de las conexiones realizadas por los usuarios para acceder a dichos recursos.

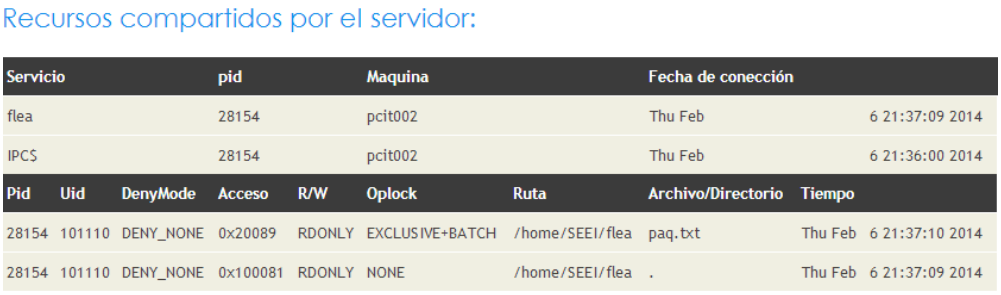

Figura 3.71 Información de monitoreo.

3.6.2.6. Módulo de Servidores

Dentro de este módulo se mostrara información sobre los sistemas Linux que han sido integrados a un domino y se encuentra dentro de la base de datos del sistema, dentro

de esta base se guardara toda la información sobre el sistema para luego ser empleada y mostrada, la información mostrada es la siguiente:

- Nombre de domino
- Dirección IP
- Información del enlace
- Información del domino
- Configuración de Integración
- Configuración de Autenticación
- Servidores NTP
- Servidores DNS

Servidores Enlazados:

Nombre: filesrv1.seei.com	
IP	192.168.0.210
Enlazado	SI
Informacion del Dominio	
LDAP server	192.168.0.100
LDAP server name	dcsrv1.seei.com
Realm	SEEI.COM
Bind Path	dc=SEEI,dc=COM
LDAP port	389
KDC server	192.168.0.100
Configuración de integración	
Dominio Winbind	SEEI
ADS realm	SEEI.COM
Comtrolador de domino	DCSRV1.SEEI.COM
Configuración de auntenticaón	
Dominio	SEEI.COM
Controlador de dominio	DCSRV1.SEEI.COM
NTP	
192.168.0.100	
0.rhel.pool.ntp.org	
DNS	
192.168.0.100	
192.168.0.1	

1 2

Figura 3.72 Información del sistema.

CAPÍTULO 4

4. Pruebas y funcionalidad de implementación

La herramienta web fue desarrollada para brindar una facilidad en la configuración y permitir una escalabilidad sistemas Linux y Windows, de esta forma la herramienta seguirá siendo útil durante mucho tiempo.

El principal recurso que puede ser compartido a los usuarios del dominio es de almacenamiento o espacio en disco, lo cual puede ser configurado gracias al servicio de Samba. Los sistemas Linux integrados al dominio pueden funcionar como servidores de archivos en los cuales almacenar la información tanto de usuarios como de la empresa.

Por defecto el directorio home del usuario se encuentra compartido en la configuración de samba, lo cual se puede notar en la Fig. 4.1.

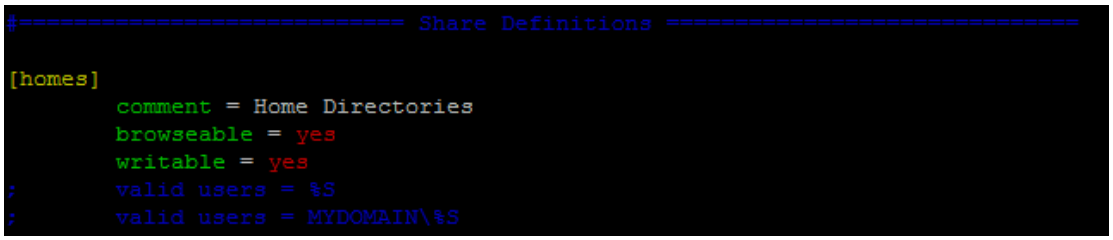

Fig. 4.1 Directorio home compartido

Cuando un usario dentro de un cliente Windows accede al sistema Linux atravez de red podrá tener acceso a una carpeta que le pertenece a el dentro del este.

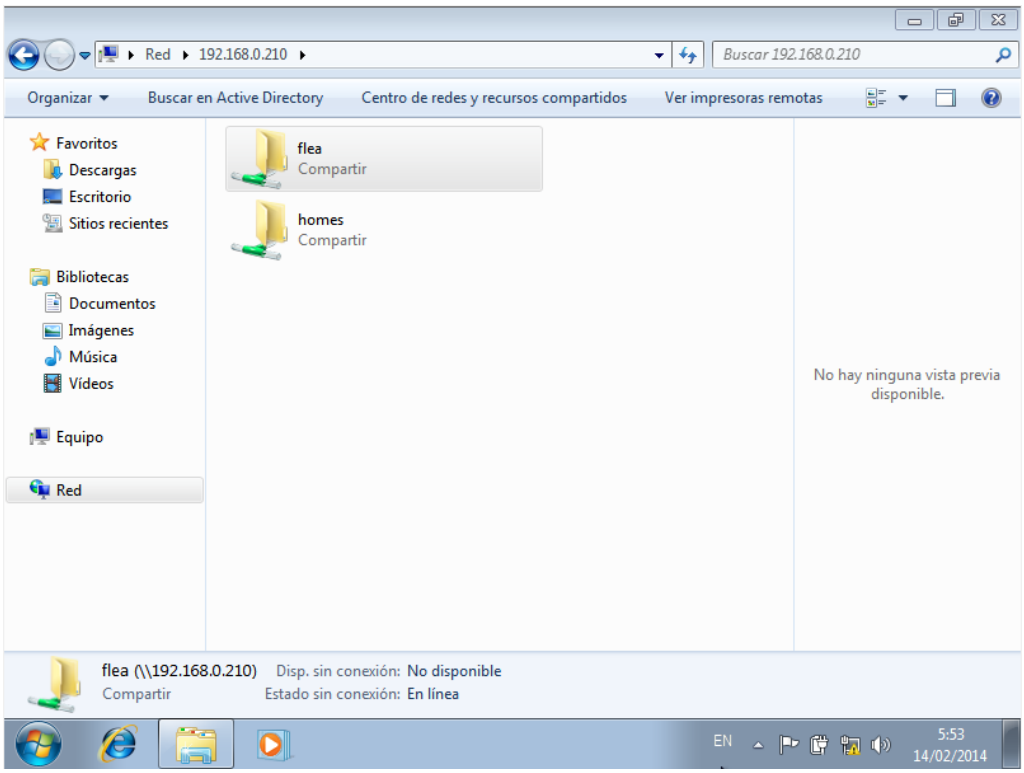

Fig. 4.2 ingreso al sistema Linux atravez de red

Dentro de esta carpeta tendrá todos los permisos de lectura y escritura. En la Fig. 4.3 se muestra la creación de un archivo y la escritura dentro de este por parte de un usuario del dominio.

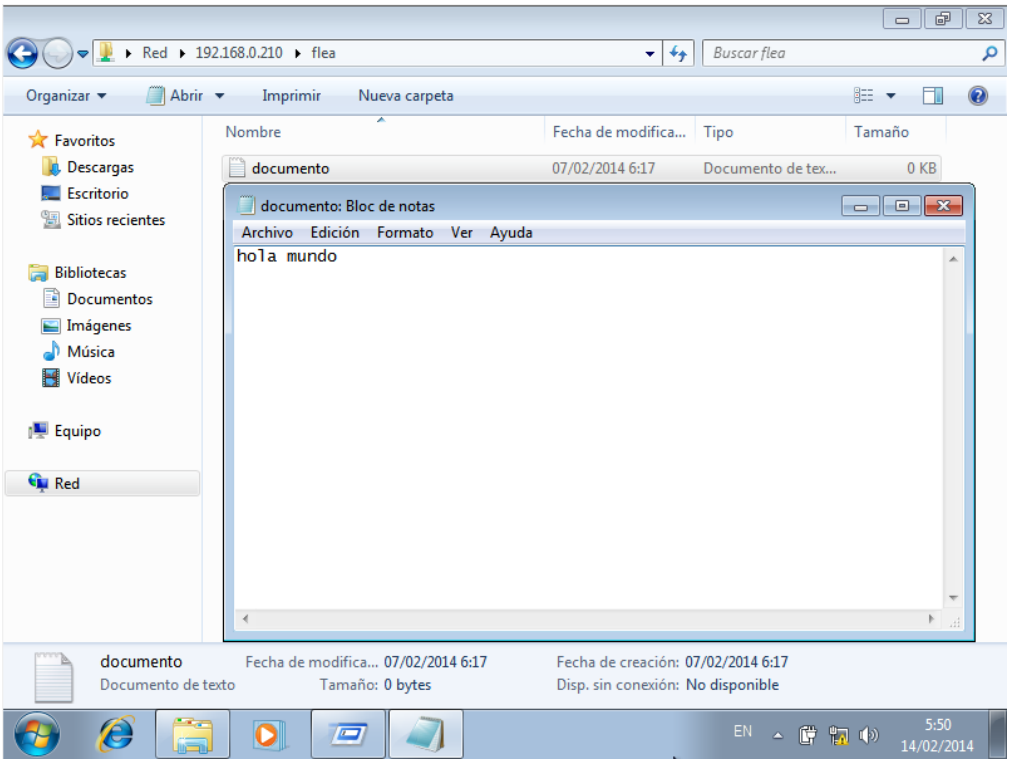

Fig. 4.3 Creacion de un archivo dentro del sistema Linux

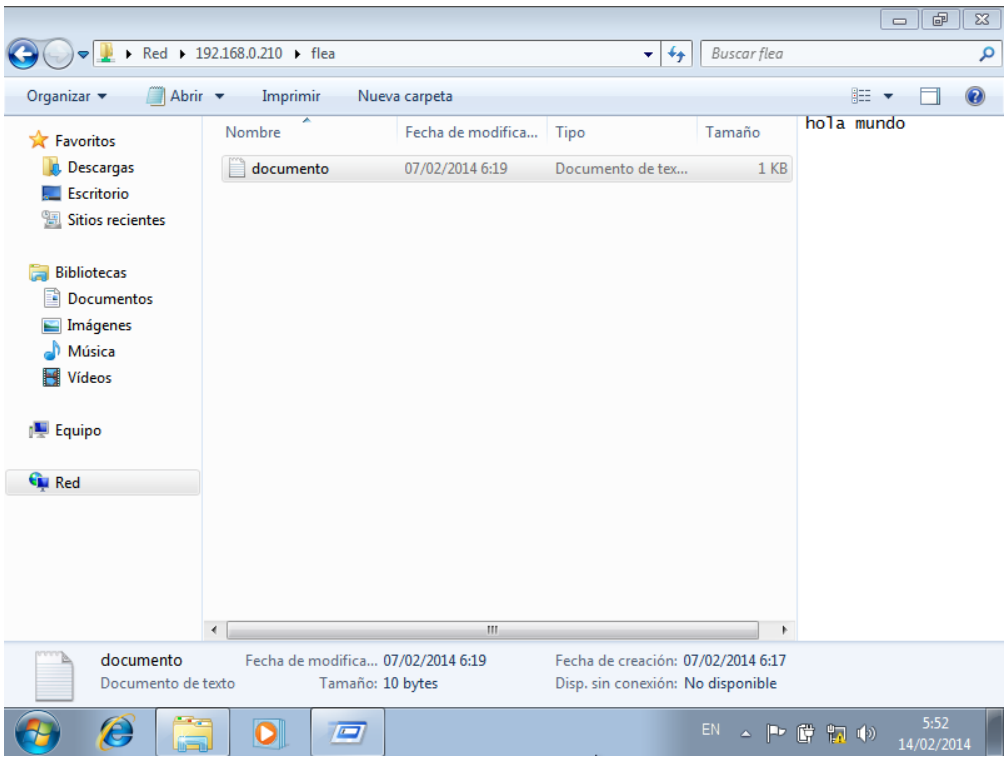

Fig. 4.4 Archivo guardado dentro del sistema Linux

Una manera de compartir un recurso dentro del sistema Linux se muestra en la siguiente figura, en esta se configura un recurso para que sea accedida por usuarios del dominio.

```
#============================ Share Definitions ==============================

[homes]
        comment = Home Directories
        browseable = yes
        writable = yes
;       valid users = %S
;       valid users = MYDOMAIN\%S

[ad-archivos]
        comment = FILESRV1 archivos del domino
        path=/ad-archivos
        writeable = yes
        browseable = yes
        valid users = %U
        guest ok = no
```

Fig. 4.5 Comparticion de recursos con ususairos del dominio

Un usuario dentro de un cliente Windows podrá acceder a este recurso y tener permisos de escritura y de lectura dentro de este.

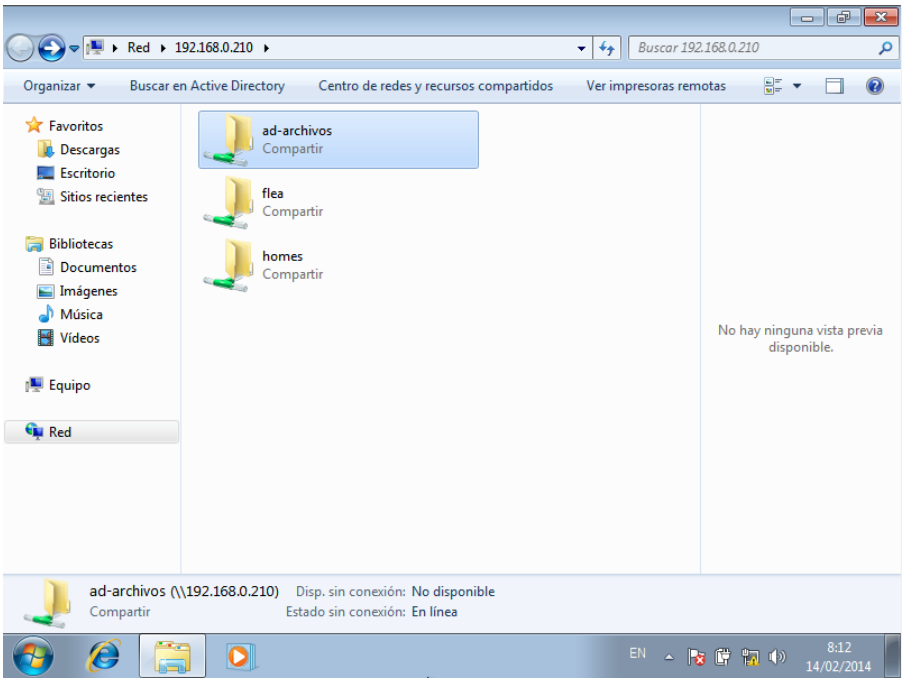

Fig. 4.6 Nuevo recurso compartido

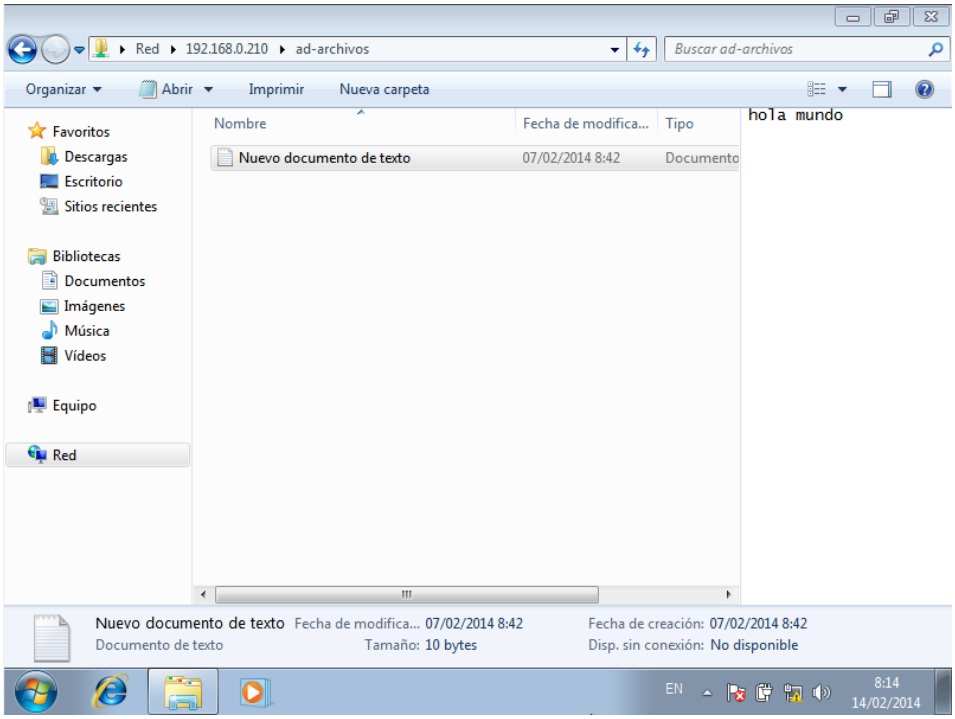

Fig. 4.7 Acceso al nuevo recurso

4.1. Escalabilidad de usuarios Windows

Los usuarios del domino podrán acceder a todos los recursos que el sistema Linux se encuentra compartiendo. Mediante la configuración normal de Samba.

Cualquier nuevo usuario que sea agregado al dominio podrá acceder tendrá acceso a estos recursos compartidos y gracias a la elección del idmap RID el sistema Linux puede formar parte de un forest o de múltiples domains trees AD, con una configuración adicional para soportalo. Por lo tanto la integración del sistema no dejara de funcionar si el diseño del AD crece.

4.2. Escalabilidad de servidores Linux

No existe un límite de integraciones ni una configuración previa para soportar la aplicación en cada sistema que se desee integrar, solo se debe instalar una vez y acceder a cada servidor que será parte del dominio mediante la sección ssh que se establece en la ventana de login.

La herramienta solo requiere ser instalada una vez y al ser web se puede acceder a ella desde cualquier equipo.

4.3. Corrección de errores

Durante el desarrollo de la aplicación se fueron corrigiendo muchos errores, tales como ejecución de comandos y manejo de información. Actualmente cara error ocurrido en la aplicación muestra al usuario un mensaje.

Los errores de ejecución que se muestran nos dan información sobre en qué parte del cada módulo ocurrió, y por qué sucedió el fallo de la aplicación.

4.4. Mejores Prácticas

Durante el desarrollo de la aplicación se explicó el funcionamiento en cada módulo y las características que poseían además de las funciones que realizaban para poder integrar el sistema Linux al dominio.

A continuación ce mostrara una lista de las mejores prácticas para emplear la aplicación:

- Para realizar toda la configuración ingresar a la aplicación como un usuario del grupo root.
- Configurar los servicios del modulo de Host previamente a cualquier otra configuración
- La aplicación no instala las dependencias de los paquetes que serán instalados mediante el link instalar
- Una vez instalado un paquete mediante la aplicación, se debe salir y entrar otra vez para poder apreciar el cambio
- Desactivar el SElinux durante el proceso de integración

CONCLUSIONES Y RECOMENDACIONES

La integración de los sistemas Windows y Linux permite crear un sistema homogéneo en donde el acceso a todos los recursos tanto en Windows como en Linux, se basa en la autenticación de usuario y aplicación de políticas de seguridad, lo cual se administra de una manera centralizada y en forma jerárquica mediante el servicio de Active Directory de Windows.

La extensión de este servicio dentro del sistema Linux mediante la implementación una herramienta que permite configurar los paquetes y servicios encargados de integrar el sistema al dominio Windows permite aumentar la escalabilidad y funcionalidad de los sistemas mixtos (Windows y Linux).

Se pueden emplear otro tipo de configuración en Samba o emplear otros servicios para una adecuada interacción entre el dominio Windows y el sistema Linux, todo depende de los requisitos y necesidades de la empresa.

En este caso se empleaba un ambiente general en el que la administración de usuarios debía seguir centralizada en el dominio y permitir el acceso a esos usuarios a recursos como espacio de almacenamiento o archivos.

Es recomendable seguir los siguientes puntos como consideraciones a tener para la integración y uso de la herramienta:

- La instalación de todos los paquetes y servicios mencionados sea solo atreves del DVD de instalación de CentOS 6, para mantener una compatibilidad entre versiones de paquetes, lo cual puede ocasionar inconvenientes

  La siguiente es una lista de los paquetes y versiones empleadas en el desarrollo de la integración:

  - samba-3.5.4-68.el6.x86_64.rp
  - samba-common-3.5.4-68.el6.x86_64.rpm
  - samba-client-3.5.4-68.el6.x86_64.rpm
  - samba-winbind-3.5.4-68.el6.x86_64.rpm
  - samba-winbind-clients-3.5.4-68.el6.x86_64.rpm
  - krb5-workstation-1.8.2-3.el6.x86_64.rpm
  - oddjob-mkhomedir-0.30-1.el6.x86_64.rpm
  - php-5.3.2-6.e16.x86_64.rpm
  - libssh2-1.2.2-7.llx86_64.rpm
  - ssh2-0.11.3
- La conexión al sistema Linux emplea el servicio ssh para autenticar a los usuarios, por lo tanto es necesarios realizar unas modificación en el servicio para permitir una rápida autenticación, modificando el

archivo /etc/ssh/sshd_config. De lo contrario se encontrar problemas como demoras en respuesta por parte de la aplicación.

  - Deshabilitar la opción de UseDNS
    - UseDNS no
  - Deshabilitar la opción GSSAPIAuthentication
    - GSSAPIAuthenticaion no

- Que existan las reglas de firewall adecuadas para en el servidor web donde se encuentra alojada la aplicación.
- Emplear políticas de firewall que habiliten el acceso al servicio smb que se encuentra ejecutando en el sistema Linux integrado al dominio. Al integrarse al dominio eh interactuar con el Active Directory solo es necesario emplear la siguiente regla:
  - -A Firewall-1-INPUT -s 192.168.10.0/24 -m state --state NEW -m tcp -p tcp --dport 445 -j ACCEPT
  - -A Firewall-1-INPUT -s 192.168.10.0/24 -m state --state NEW -m udp -p udp --dport 445 -j ACCEPT
- Para mayor seguridad dentro de los sistemas Linux, se debe configurar adecuadamente el SELinux para habilitar los permisos de lectura y escritura en los recursos compartidos que se encuentran dentro del sistema Linux mediante Samba.

Setsebool es un comando que habilita y deshabilita la protección de SELinux, para obtener una lista de completa de las opciones de seguridad se puede emplear getsetbool.

- getsetbool –a |grep samba
- getsetbool –a | grep smb

Mediante el empleo de los comandos anteriores se puede listar una completa lista de opciones para Samba.

Para compartir el directorio home por defecto se debe emplear el siguiente comando.

- setsebool –P samba_home_dirs on

- Para que se pueda crear correctamente un registro DNS con el nombre de dominio y dirección IP del sistema Linux integrado al dominio, en el servidor DNS se debe habilitar las actualizaciones desde cualquier origen.

ANEXOS

Anexo A

Iso 27001

SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

Un Sistema de Gestión de la seguridad de la Información *(SGSI)* es, como el nombre lo sugiere, un conjunto de políticas de administración de la información. El término es utilizado principalmente por la ISO/IEC 27001.

El término se denomina en inglés "Information Security Management System" (ISMS).

El concepto clave de un SGSI es para una organización el diseño, implantación, mantenimiento de un conjunto de procesos para gestionar eficientemente la accesibilidad de la información, buscando asegurar la confidencialidad, integridad y disponibilidad de los activos de información minimizando a la vez los riesgos de seguridad de la información.

Como todo proceso de gestión, un SGSI debe seguir siendo eficiente durante un largo tiempo adaptándose a los cambios internos de la organización así como los externos del entorno.

Ello ayuda a proteger los activos de información y otorga confianza a cualquiera de las partes interesadas, sobre todo a los clientes. La norma adopta un enfoque por procesos para establecer, implantar, operar, supervisar, revisar, mantener y mejorar un SGSI.

ISO/IEC 27001 es la única norma internacional auditable que define los requisitos para un sistema de gestión de la seguridad de la información (SGSI). La norma se ha concebido para garantizar la selección de controles de seguridad adecuados y proporcionales.

Anexo B

Index.php

Codigo de la pantalla de login de la herramienta.

```
<?php
	session_start();
	if($_SESSION['autenticado']){
		header('location: Host.php');
	 }
?>
<!DOCTYPE html>
<html lang="es">
	<head>
		<meta charset="utf-8"/>
		<meta http-equiv="content-type" content="text/html; charset=windows-1252"
/>
		<link rel="stylesheet" type="text/css" href="style/style.css" title="style" />
		<script type="text/javascript" src="style/script.js"></script>
		<title>Integraci&oacute;n</title>
	</head>
	<body id="body_login">
		<div id="login_content">
			<div id="login">
				<form action="functions/validar_usuario.php" method="post"
enctype="application/x-www-form-urlencoded" onsubmit="return login(this);">
					<div class="form_login">
						<h2>Bienvenido</h2>
						<p><input name="admin"
placeholder="Usuario" required="required" type="text"/></p>
						<p><input name="password_usuario"
placeholder="Contrase&ntilde;a" required="required" type="password"/></p>
						<p><input  name="servidor" placeholder="IP
Servidor" required="required" type="text" value="<?php  echo gethostname();?>"/></p>
						<p><span> </span><input
class="submit" name="iniciar" type="submit" value="Login"/></p>
						<?php
							 if($_GET['error_login']=="yes"){
							echo "<span id=\"error_login\"
>Error de autenticaci&oacute;n</span>";}
						?>
					</div>
				</form>
			</div>
		</div>
	</body>
</html>
```

Autenticar.php

Codigo de pantalla de autenticación.

```
<?php
  session_start();
  if(!$_SESSION['autenticado']){
    header('location: index.php');
    exit;
  }
        if(!$_SESSION['requisitos'] || !$_SESSION['root_group']){
                header ('Location: Info.php');
        }
        include 'functions/servers.php';
        include 'functions/funciones_db.php';
?>

<!DOCTYPE html>
<html>
  <head>
    <meta charset="utf-8"/>
                <meta http-equiv="content-type" content="text/html; charset=windows-1252"
/>
                <link rel="stylesheet" type="text/css" href="style/style.css" title="style" />
                <script type="text/javascript" src="style/script.js"></script>
          <title>Integraci&oacute;n</title>
  </head>
  <body>
                <div id="main">
                        <div id="header">
                                <div id="logo-img"><img src="style/espol-logo.gif" alt="logo"
/></div>
        <div id="session-user">
          <h2>Servidor: <?php echo $_SESSION['hostname']?></h2>
          <h2>Usuario: <?php echo $_SESSION['usuario']?></h2>
          <p><a href="functions/logout.php">SALIR</a></p>
        </div>
                                <div id="logo">
                                        <div id="logo_text">
                                                <h1><a href="Host.php">Inter<span
class="logo_colour">operabilidad</span></a></h1>
                                                <h2>Interoperabilidad y compartici&oacute;n
de recursos entre dominios Active Directory y servidores Linux</h2>
                                                <h2><noscript><img id="alert"
src="style/warning.png">Para un correcto funcionamiento de la aplicaci&oacute;n habilitar
javascript en su navegador!</noscript></h2>
                                                <?php
                                                        if(!$_SESSION['root_group']){
                                                                echo "<h2><img id=\"alert\"
src=\"style/warning.png\">El usuario no esta habilitado para realizar configuraciones en el
sistema!</h2>";
```

```
                                                }
                                        ?>
                                </div>
                        </div>
                        <div id="menubar">
                                <ul id="menu">
                                <li><a href="Host.php">HOST</a></li>
                                <li><a
href="Autenticar.php">AUTENTICACI&Oacute;N</a></li>
                                <li><a
href="Integrar.php">INTEGRACI&Oacute;N</a></li>
                                <li><a
href="Info.php">INFORMACI&Oacute;N</a></li>
                                <li><a href="Servidores.php">SERVIDORES</a></li>
                                </ul>
                        </div>
                </div>
                <div id="site_content">
                        <div id="content">
                                <div class="info">
                                        <div class="show_info">
                                                <h3>Kerberos</h3>
                                                <h4>Protocolo de
autenticaci&oacute;n</h4>
                                                <p>Permite a dos computadores en
una red insegura demostrar su identidad mutuamente de manera segura.</p>
                                        </div>
                                        <h2>Configuraci&oacute;n de Kerberos</h2>
                                </div>
                                <form action="functions/kerberos.php"
method="post" enctype="application/x-www-form-urlencoded" onsubmit="return
kerberos(this);" >
                                        <div class="form_settings">
                                                <div class="info">
                                                        <div class="show_info">
                                                                <h3>Dominio</h3>
                                                                <h4>Windows
Active Directory Domain</h4>
                                                                <p>Red de
computadoras en la cual usarios, computadoras, impresoras y politicas de seguridad estan
registrados en una base central llamada Directory Service</p>
                                                                <h5>Ingrese el
Dominio Active Directory al cual desea acceder</h5>
                                                        </div>

        <p><span>Dominio:</span><input type="text" name="domain"
placeholder="EJEMPLO.COM"  value="<?php echo $_GET['edi_dom'];?>"/></p>
                                                </div>
                                                <div class="info">
                                                        <div class="show_info">
```

```
                                                                    <h3>Controlador de
Dominio</h3>
                                                                    <h4>Domain
Controler (DC)</h4>
                                                                    <p>Permite o
deniega el acceso a un dominio y sus recursos de red</p>
                                                                    <h5>Ingrese el
Controlador de Dominio del Dominio Active Directory</h5>
                                                                </div>
                                                                <p><span>Controlador de
Dominio:</span><input type="text" name="dc" placeholder="SRV_DC.EJEMPLO.COM"
value="<?php echo $_GET['edi_dc'];?>"/></p>
                                                            </div>
                                                            <p><span> </span><input
class="submit" type="submit" name="submit" value="Agregar" /></p>
                                                        </div>
                                                </form>
                                                <?php
                                                        $servers=domain();
                                                        krb_db('functions/Integracion.db',
$servers[0], $servers[1]);
                                                        echo "<table>";
                                                        echo "<caption>Dominio</caption>";
                                                        echo "<tbody>";
                                                        echo
"<tr><th>Dominio</th><th>Controlador de dominio</th></tr>";
                                                        echo "<tr>";
                                                        foreach($servers as $server){
                                                                if($server!=""){
                                                                        echo "<td>".$server."</td>";
                                                                }
                                                        }
                                                        echo "<td><a
href=\"functions/eliminar_kerberos.php?server=".$server."\">Reset</a></td>";
                                                        echo "<td><a
href=\"Autenticar.php?edi_dom=".$servers[0]."&edi_dc=".$servers[1]."\">Editar</a></td>";
                                                        echo "</tr>";
                                                        echo "</tbody>";
                                                        echo "</table>";
                                                ?>
                                        </div>
                                </div>
                                <div id="footer">
                                        Proyecto de grado de Lic. en Redes y Sistemas Operativos | <a
href="http://espol.edu.ec">ESPOL</a>
                                </div>
                        </div>
                        <?php
                                if($_GET['error']){
                                        echo "<div id=\"mensaje\" class=\"mensaje_main\">";
                                        echo "<div class=\"mensaje\">";
```

```
                        }
                        if($_GET['error']=="krb1"){
                                echo "<h2 class=\"error\" >No se pudo agregar el servidor de
autenticaci&oacute;n</h2>";
                        }if($_GET['error']=="krb2"){
                                echo "<h2 class=\"error\" >No se pudo editar el DNS</h2>";
                        }
                        if($_GET['error']=="krb0"){
                                echo "<h2 class=\"error\" >Ingrese valores validos!</h2>";
                        }
                        if($_GET['error']){
                                echo "<div id=\"div_button\">";
                                echo "<button id=\"button\"
onClick=\"ocultar()\">Aceptar</button>";
                                echo "</div>";
                                echo "</div>";
                                echo "</div>";
                        }
                ?>
  </body>
</html>
```

Host.php

Codigo de la pantalla de host.

```
<?php
  session_start();
  if(!$_SESSION['autenticado']){
    header('location: index.php');
    exit;
  }
        if(!$_SESSION['requisitos'] || !$_SESSION['root_group']){
                header ('Location: Info.php');
        }
        include 'functions/servers.php';
        include 'functions/funciones_db.php';
?>
<!DOCTYPE html>
<html>
  <head>
    <meta charset="utf-8"/>
                <meta http-equiv="content-type" content="text/html; charset=windows-1252"
/>
                <link rel="stylesheet" type="text/css" href="style/style.css" title="style" />
                <script type="text/javascript" src="style/script.js"></script>
          <title>Integraci&oacute;n</title>
                </script>
  </head>
  <body>
```

```
                <div id="main">
                        <div id="header">
                                        <div id="logo-img"><img src="style/espol-logo.gif"
alt="logo" /></div>
                <div id="session-user">
                  <h2>Servidor: <?php echo $_SESSION['hostname']?></h2>
                  <h2>Usuario: <?php echo $_SESSION['usuario']?></h2>
                  <p><a href="functions/logout.php">SALIR</a></p>
                </div>
                                        <div id="logo">
                                                <div id="logo_text">
                                                        <h1><a href="Host.php">Inter<span
class="logo_colour">operabilidad</span></a></h1>
                                                        <h2>Interoperabilidad y
compartici&oacute;n de recursos entre dominios Active Directory y servidores Linux</h2>
                                                        <h2><noscript><img id="alert"
src="style/warning.png">Para un correcto funcionamiento de la aplicaci&oacute;n habilitar
javascript en su navegador!</noscript></h2>
                                                        <?php
                                                                if(!$_SESSION['root_group']){
                                                                        echo "<h2><img
id=\"alert\" src=\"style/warning.png\">El usuario no esta habilitado para realizar
configuraciones en el sistema!</h2>";
                                                                }
                                                        ?>
                                                </div>
                                        </div>
                <div id="menubar">
                                                <ul id="menu">
                                                        <li><a
href="Host.php">HOST</a></li>
                                                        <li><a
href="Autenticar.php">AUTENTICACI&Oacute;N</a></li>
                                                        <li><a
href="Integrar.php">INTEGRACI&Oacute;N</a></li>
                                                        <li><a
href="Info.php">INFORMACI&Oacute;N</a></li>
                                                        <li><a
href="Servidores.php">SERVIDORES</a></li>
                                                </ul>
                                        </div>
                        </div>
                        <div id="site_content">
                                <div id="content">
                                        <h2>Host</h2>
                                        <ul>
                                                <li>Hostname: <?php echo
$_SESSION['hostname']?></li>
                                                <li>IP: <?php echo $_SESSION['ip']?></li>
                                        <div  class="info">
                                                <div class="show_info">
```

```
                                                <h3>Hostname</h3>
                                                <h4>Nombre de dominio</h4>
                                                <p>Es un nombre que se asigna a un
equipo en red  para identificarlo</p>
                                                <h5>Ingrese el nombre del equipo
usando FQDN (fully qualified domain name)</h5>
                                                <h5><img id="alert"
src="style/warning.png">Cambiar REINICIARA el equipo!</h5>
                                        </div>
                                        <h2>Configuraci&oacute;n Hostname</h2>
                                        <form action="functions/hostname.php"
method="post" enctype="application/x-www-form-urlencoded" onsubmit="return host(this);">
                                                <div class="form_settings">
                                                        <p><span>Nombre de
dominio:</span><input type="text" name="nombre" placeholder="FILESRV.EXAMPLE.COM"
value="<?php echo $_SESSION['hostname'];?>" /></p>

        <p><span> </span><input class="submit" type="submit" name="submit"
value="Cambiar" /></p>
                                                </div>
                                        </form>
                                        <p></p>
                                </div>
                                <div  class="info">
                                        <div class="show_info">
                                                <h3>NTP</h3>
                                                <h4>Network Time Protocol
(NTP)</h4>
                                                <p>Protocolo de Internet para
sincronizar los relojes de los sistemas inform&aacute;ticos</p>
                                                <h5>Ingrese la IP del servidor NTP
del Dominio Active Directory</h5>
                                        </div>
                                        <h2>Configuraci&oacute;n NTP</h2>
                                        <form action="functions/ntp.php"
method="post" enctype="application/x-www-form-urlencoded" onsubmit="return ntp(this);" >
                                                <div class="form_settings">
                                                        <p><span
class="a">Servidor NTP:</span><input class="b" type="text" name="ipserver" placeholder="IP
del servidor NTP" /></p>

        <p><span> </span><input class="submit" type="submit" name="submit"
value="Agregar" /></p>
                                                </div>
                                        </form>
                                        <p></p>
                                </div>
                                <div class="info">
                                        <div class="show_info">
                                                <h3>DNS</h3>
```

```
                                                    <h4>Domain Name System (DNS)
</h4>
                                                    <p>Sistema de nomenclatura
jer&aacute;rquica para computadoras, servicios o cualquier recurso conectado a Internet o a una
red privada.</p>
                                                    <h5>Ingrese la IP del servidor DNS
del Dominio Active Directory</h5>
                                            </div>
                                            <h2>Configuraci&oacute;n DNS</h2>
                                            <form action="functions/dns.php"
method="post" enctype="application/x-www-form-urlencoded" onsubmit="return dns(this);">
                                                    <div class="form_settings">
                                                            <p><span>Servidor
DNS:</span><input type="text" name="dnsserver" placeholder="IP del servidor DNS"/></p>

        <p><span> </span><input class="submit" id="submit" type="submit"
name="submit" value="Agregar" /></p>
                                                    </div>
                                            </form>
                                            <p></p>
                                    </div>
                                    <?php
                                            $servers=servers_ntp();
                                            echo "<table>";
                                            echo "<caption>Servidores NTP</caption>";
                                            echo "<tbody>";
                                            foreach($servers as $server){
                                                    if($server!=""){
                                                            echo "<tr>
<td>".$server."</td>";
                                                            echo "<td><a
href=\"functions/eliminar_ntp.php?server=".$server."\">eliminar</a></td>";
                                                            echo "<td><a
href=\"functions/sincronizar_ntp.php?server=".$server."\">sincronizar</a></td></tr>";

        ntp_db('functions/Integracion.db',$server);
                                                    }
                                            }
                                            echo "</tbody>";
                                            echo "</table>";
                                            $servers=servers_dns();
                                            echo "<table>";
                                            echo "<caption>Servidores DNS</caption>";
                                            echo "<tbody>";
                                            foreach($servers as $server){
                                                    if($server!=""){
                                                            echo
"<tr><td>".$server."</td>";
                                                            echo "<td><a
href=\"functions/eliminar_dns.php?dnsserver=".$server."\">eliminar</a></td></tr>";
```

```
        dns_db('functions/Integracion.db',$server);
                                                        }
                                                }
                                                echo "</tbody>";
                                                echo "</table>";
                                                $db=null;
                                        ?>
                                </div>
                        </div>
                        <div id="footer">
                                Proyecto de grado de Lic. en Redes y Sistemas Operativos | <a
href=\"http://espol.edu.ec\">ESPOL</a>
                        </div>
                </div>
                <?php
                        if($_GET['error']){
                                echo "<div id=\"mensaje\" class=\"mensaje_main\">";
                                echo "<div class=\"mensaje\">";
                        }
                        if($_GET['error']=="dns1"){
                                echo "<h2 class=\"error\" >No se pudo agregar el DNS</h2>";
                        }if($_GET['error']=="dns2"){
                                echo "<h2 class=\"error\" >No se pudo eliminar el DNS</h2>";
                        }
                        if($_GET['error']=="ntp1"){
                                echo "<h2 class=\"error\" >No se puede acceder al servicio
NTP</h2>";
                        }if($_GET['error']=="ntp2"){
                                echo "<h2 class=\"error\" >No se puede sincronizar con el
servidor NTP</h2>";
                        }if($_GET['error']=="ntp3"){
                                echo "<h2 class=\"error\" >No se puede agregar el
servidor</h2>";
                        }if($_GET['error']=="ntp4"){
                                echo "<h2 class=\"error\" >No se puede iniciar el servicio
NTP</h2>";
                        }if($_GET['error']=="ntp5"){
                                echo "<h2 class=\"error\" >No se puede eliminar el
servidor</h2>";
                        }if($_GET['error']=="ntp_yes"){
                                echo "<h2>Sincronizaci&oacute;n exitosa</h2>";
                        }
                        if($_GET['error']=="host1"){
                                echo "<h2 class=\"error\" >No se puede cambiar el
Nombre/h2>";
                        }
                        if($_GET['error']=="dns0" || $_GET['error']=="ntp0" ||
$_GET['error']=="host0"){
                                echo "<h2 class=\"error\" >Ingrese un valor valido!</h2>";
                        }
```

```
                        if($_GET['error']){
                                echo "<div id=\"div_button\">";
                                echo "<button id=\"button\"
onClick=\"ocultar()\">Aceptar</button>";
                                echo "</div>";
                                echo "</div>";
                                echo "</div>";
                        }
                ?>
  </body>
</html>
```

Integrar.php

Codigo de la pantalla integración.

```
<?php
  session_start();
  if(!$_SESSION['autenticado']){
    header('location: index.php');
    exit;
  }
        if(!$_SESSION['requisitos'] || !$_SESSION['root_group']){
                header ('Location: Info.php');
        }
  if($_SESSION['dominio']){
    $wd=$_SESSION['wd'];
    $war=$_SESSION['war'];
    $wdc=$_SESSION['wdc'];
  }
        include 'functions/servers.php';
        include 'functions/funciones_db.php';
?>

<!DOCTYPE html>
<html lang="en">
  <head>
    <meta charset="utf-8" />
                <meta http-equiv="content-type" content="text/html; charset=windows-1252"
/>
                <link rel="stylesheet" type="text/css" href="style/style.css" title="style" />
                <script type="text/javascript" src="style/script.js"></script>
    <title>Integraci&oacute;n</title>
  </head>
  <body>
                <div id="main">
                        <div id="header">
                                <div id="logo-img"><img src="style/espol-logo.gif" alt="logo"
/></div>
```

```
<div id="session-user">
  <h2>Servidor: <?php echo $_SESSION['hostname']?></h2>
  <h2>Usuario: <?php echo $_SESSION['usuario']?></h2>
  <p><a href="functions/logout.php">SALIR</a></p>
</div>
                        <div id="logo">
                                <div id="logo_text">
                                        <h1><a href="Host.php">Inter<span
class="logo_colour">operabilidad</span></a></h1>
                                        <h2>Interoperabilidad y compartici&oacute;n
de recursos entre dominios Active Directory y servidores Linux</h2>
                                        <h2><noscript><img id="alert"
src="style/warning.png">Para un correcto funcionamiento de la aplicaci&oacute;n habilitar
javascript en su navegador!</noscript></h2>
                                        <?php
                                                if(!$_SESSION['root_group']){
                                                        echo "<h2><img id=\"alert\"
src=\"style/warning.png\">El usuario no esta habilitado para realizar configuraciones en el
sistema!</h2>";
                                                }
                                        ?>
                                </div>
                        </div>
                                <div id="menubar">
                                        <ul id="menu">
                                                <li><a
href="Host.php">HOST</a></li>
                                                <li><a
href="Autenticar.php">AUTENTICACI&Oacute;N</a></li>
                                                <li><a
href="Integrar.php">INTEGRACI&Oacute;N</a></li>
                                                <li><a
href="Info.php">INFORMACI&Oacute;N</a></li>
                                                <li><a
href="Servidores.php">SERVIDORES</a></li>
                                        </ul>
                                </div>
                        </div>
                        <div id="site_content">
                                <div id="content">
                                        <div class="info">
                                                <div class="show_info">
                                                        <h3>SAMBA</h3>
                                                        <h4>Implementaci&oacute;n libre de
los protocolos de red SMB/CISF</h4>
                                                        <p>Provee archivos y servicios de
impreci&oacute;n a clientes Windows, se puede integrar como un Dominio Windows Server,
tambien como un Primary Domain Controler o como miembro de Dominio, y tambiem puede ser
parte de un Dominio Active Directory</p>
                                                        <h4>Winbind</h4>
```

```
                                                    <p>Componente de SAMBA que
resuelve los problemas de la unificaci&oacute;n de logon. Usa una implementaci&oacute;n de
Microsoft RPC calls,  Pluggable Authentication Modules (PAMs), y el  Name Service Switch (NSS)
para permitir a usuarios de Dominio WIndows aparecer y operar como usuarios UNIX en
maquinas UNIX</p>
                                                </div>
                                                <h2>Configuraci&oacute;n de
Samba/Winbind</h2>
                                            </div>
                                            <form action="functions/authconfig.php"
method="post" enctype="application/x-www-form-urlencoded" onsubmit="return
samba_winbind(this);">
                                                <div class="form_settings">
                                                    <div class="info">
                                                        <div class="show_info">
                                                            <h3>Dominio
Winbind</h3>
                                                            <h4>Windows
Active Directory Domain</h4>
                                                            <p>Red de
computadoras en la cual usarios, computadoras, impresoras y politicas de seguridad estan
registrados en una base central llamada Directory Service</p>
                                                            <h5>Ingrese el
Dominio Active Directory al cual desea integrarse</h5>
                                                        </div>
                                                        <p><span>Dominio
Winbind</span><input type="text" name="wd" placeholder="EJEMPLO" value="<?php echo
$wd;?>"/></p>
                                                    </div>
                                                    <div class="info">
                                                        <div class="show_info">
                                                            <h3>ADS
Realm</h3>
                                                            <h4>Active
Directory Server Realm</h4>
                                                            <p>Especifica el
campo donde el servidor SAMBA actuara como mienbro de dominio</p>
                                                            <h5>Ingrese el
Dominio Active Directory al cual desea acceder</h5>
                                                        </div>
                                                        <p><span>ADS
Realm</span><input type="text" name="war" placeholder="EJEMPLO.COM"  value="<?php echo
$war;?>"/></p>
                                                    </div>
                                                    <div class="info">
                                                        <div class="show_info">
                                                            <h3>Controlador de
Dominio</h3>
                                                            <h4>Domain
Controler (DC)</h4>
```

```
                                                                <p>Permite o
deniega el acceso a un dominio y sus recursos de red</p>
                                                                <h5>Ingrese el
Controlador de Dominio del Dominio Active Directory</h5>
                                                        </div>
                                                        <p><span>Controlador de
dominio</span><input type="text" name="wdc" placeholder="SRV_DC.EJEMPLO.COM"
value="<?php echo $wdc;?>"/></p>
                                                </div>
                                                <div class="info">
                                                        <div class="show_info">

        <h4>Administrador</h4>
                                                                <h5>Ingrese el
usuario administrador del Contorlador de Dominio Active Directory </h5>
                                                        </div>

        <p><span>Administrador:</span><input name="adm"  type="text"/></p>
                                                </div>
                                                <div class="info">
                                                        <div class="show_info">

        <h4>Contrase&ntilde;a</h4>
                                                                <h5>Ingrese el la
contrase&ntilde;a del Admnistrador del Controlador de Dominio Active Directory</h5>
                                                        </div>

        <p><span>Contrase&ntilde;a:</span><input name="password_adm"
type="password"/></p>
                                                </div>
                                                <p><span> </span><input
class="submit" type="submit" name="submit" value="Agregar" /></p>
                                        </div>
                                </form>
                                <?php
                                        $var=dominio_winbind();
                                        $wd1=$var['wd'];
                                        $war1=$var['war'];
                                        $wdc1=$var['wdc'];
                                        $enlazado="NO";
                                        if($_SESSION['enlazado']){
                                                $enlazado="SI";
                                        }
                                        sw_db('functions/Integracion.db', $var['wd'],
$var['war'], $var['wdc']);
                                        echo "<h2>Enlazado al Dominio:
".$enlazado."</h2>";
                                        echo "<table>";
                                        echo "<caption>Cunfiguraci&oacute;n de
autenticaci&oacute;n</caption>";
                                        echo "<tbody>";
```

```
                                                echo "<tr><th>Dominio
Winbind</th><td>".$wd1."</td></tr>";
                                                echo "<tr><th>ADS
Realm</th><td>".$war1."</td></tr>";
                                                echo "<tr><th>Controlador de
dominio</th><td>".$wdc1."</td></tr>";
                                                echo "</tbody>";
                                                echo "</table>";
                                        ?>
                                </div>
                        </div>
                </div>
                <div id="footer">
                        Proyecto de grado de Lic. en Redes y Sistemas Operativos | <a
href=\"http://espol.edu.ec\">ESPOL</a>
                </div>
                <?php
                        if($_GET['error']){
                                echo "<div id=\"mensaje\" class=\"mensaje_main\">";
                                echo "<div class=\"mensaje\">";
                        }
                        if($_GET['error']=="dk_yes"){
                                echo "<h2>Kerberos y DNS Actualizado!</h2>";
                        }
                        if($_GET['error']=="auth_yes"){
                                $_SESSION['wd']="";
                                $_SESSION['war']="";
                                $_SESSION['wdc']="";
                                echo "<h2>Enlazado al dominio con exito!</h2>";
                        }if($_GET['error']=="auth2"){
                                $_SESSION['wd']="";
                                $_SESSION['war']="";
                                $_SESSION['wdc']="";
                                echo "<h2 class=\"error\" >NO se pudo enlazar al nuevo
dominio!</h2>";
                        }if($_GET['error']=="auth1"){
                                $_SESSION['wd']="";
                                $_SESSION['war']="";
                                $_SESSION['wdc']="";
                                echo "<h2 class=\"error\" >NO se pudo enlazar al
dominio!</h2>";
                        }
                        if($_GET['error']=="auth0"){
                                echo "<h2 class=\"error\" >Ingrese valores validos!</h2>";
                        }
                        if($_GET['error']){
                                echo "<div id=\"div_button\">";
                                echo "<button id=\"button\"
onClick=\"ocultar()\">Aceptar</button>";
                                echo "</div>";
                                echo "</div>";
```

```
                                        echo "</div>";
                                }
                        ?>
  </body>
</html>
```

Info.php

Codigo de la pantalla de información.

```
<?php
  session_start();
  if(!$_SESSION['autenticado']){
    header('location: index.php');
    exit;
  }
  include 'functions/servers.php';
        include 'functions/funciones_db.php';
?>

<!DOCTYPE html>
<html>
  <head>
    <meta charset="utf-8"/>
                <meta http-equiv="content-type" content="text/html; charset=windows-1252"
/>
          <link rel="stylesheet" type="text/css" href="style/style.css" title="style" />
                <script type="text/javascript" src="style/script.js"></script>
                <script type="text/javascript">
                        var myVar=setInterval(function(){recursos()},400);
                        function recursos(){
                                var xmlhttp=new XMLHttpRequest();

                                xmlhttp.onreadystatechange=function(){
                                        if (xmlhttp.readyState==4 && xmlhttp.status==200){

        document.getElementById("tabla").innerHTML=xmlhttp.responseText;
                                  }
                                }
                        xmlhttp.open("GET","functions/monitoreo.php",true);
                        xmlhttp.send();
                        }
                </script>
          <title>Integraci&oacute;n</title>
  </head>
  <body onload="recursos();">
                <div id="main">
                        <div id="header">
                                <div id="logo-img"><img src="style/espol-logo.gif" alt="logo"
/></div>
```

```
<div id="session-user">
  <h2>Servidor: <?php echo $_SESSION['hostname']?></h2>
  <h2>Usuario: <?php echo $_SESSION['usuario']?></h2>
  <p><a href="functions/logout.php">SALIR</a></p>
</div>
                        <div id="logo">
                                <div id="logo_text">
                                        <h1><a href="app.php">Inter<span
class="logo_colour">operabilidad</span></a></h1>
                                        <h2>Interoperabilidad y compartici&oacute;n
de recursos entre dominios Active Directory y servidores Linux</h2>
                                        <h2><noscript><img id="alert"
src="style/warning.png">Para un correcto funcionamiento de la aplicaci&oacute;n habilitar
javascript en su navegador!</noscript></h2>
                                        <?php
                                                if(!$_SESSION['root_group']){
                                                        echo "<h2><img id=\"alert\"
src=\"style/warning.png\">El usuario no esta habilitado para realizar configuraciones en el
sistema!</h2>";
                                                }
                                        ?>
                                </div>
                        </div>
                        <div id="menubar">
                                <ul id="menu">
                                        <li><a href="Host.php">HOST</a></li>
                                        <li><a
href="Autenticar.php">AUTENTICACI&Oacute;N</a></li>
                                        <li><a
href="Integrar.php">INTEGRACI&Oacute;N</a></li>
                                        <li><a
href="Info.php">INFORMACI&Oacute;N</a></li>
                                        <li><a
href="Servidores.php">SERVIDORES</a></li>
                                </ul>
                        </div>
                </div>
                <div id="site_content">
                        <div id="content_info">
                                <?php
                                        echo "<h2>Paquetes instalados en el
Host:</h2>";
                                        $versiones=$_SESSION['paquetes'];
                                        $nombres=array('Samba','Samba-
Common','Samba-Client','Samba-Winbind','Samba-Winbind-Clients','Krb5-Workstation','Oddjob-
Mkhomedir');
                                        echo "<table>";
                                                echo "<tbody>";
                                                echo
"<tr><th>Paquete</th><th>Informaci&oacute;n</th><th></th></tr>";
                                                for($i=0;$i<7;$i++){
```

```
                                                                    echo
"<tr><td>".$nombres[$i]."</td>";

        $var=strpos($versiones[$i],"is not installed");
                                                                    if($var){
                                                                            echo "<td>NO
instalado</td>";

        if($_SESSION['root_group']){
                                                                                    echo
"<td><a href=\"functions/instalar.php?paquete=".$i."\">Instalar</a></td></tr>";
                                                                            }else{
                                                                                    echo
"</tr>";
                                                                            }
                                                                    }else{
                                                                            echo
"<td>".$versiones[$i]."</td><td></td></tr>";
                                                                    }
                                                            }
                                                            echo "</tbody>";
                                                    echo "</table>";
                                            ?>
                                            <div id="tabla"></div>
                                    </div>
                            </div>
                            <div id="footer">
                                    Proyecto de grado de Lic. en Redes y Sistemas Operativos | <a
href=\"http://espol.edu.ec\">ESPOL</a>
                            </div>
                    </div>
                    <?php
                            if($_GET['error']){
                                    echo "<div class=\"mensaje_main\">";
                                    echo "<div class=\"mensaje\">";
                            }
                            if($_GET['error']=="pak1"){
                                    echo "<h2 class=\"error\">NO se pudo instalar el
paquete</h2>";
                            }
                            if($_GET['error']){
                                    echo "<div id=\"div_button\">";
                                    echo "<a id=\"button\" href=\"Info.php\">Aceptar</a>";
                                    echo "</div>";
                                    echo "</div>";
                                    echo "</div>";
                            }
                    ?>
        </body>
</html>
```

Servidores.php

Codigo de la pantalla de servidores.

```
<?php
  session_start();
  if(!$_SESSION['autenticado']){
    header('location: index.php');
    exit;
  }
  include 'functions/servers.php';
        include 'functions/funciones_db.php';
?>

<!DOCTYPE html>
<html>
  <head>
    <meta charset="utf-8"/>
                <meta http-equiv="content-type" content="text/html; charset=windows-1252"
/>
          <link rel="stylesheet" type="text/css" href="style/style.css" title="style" />
                <script type="text/javascript" src="style/script.js"></script>

          <title>Integraci&oacute;n</title>
  </head>
  <body>
                <div id="main">
                      <div id="header">
                            <div id="logo-img"><img src="style/espol-logo.gif" alt="logo"
/></div>
        <div id="session-user">
          <h2>Servidor: <?php echo $_SESSION['hostname']?></h2>
          <h2>Usuario: <?php echo $_SESSION['usuario']?></h2>
          <p><a href="functions/logout.php">SALIR</a></p>
        </div>
                            <div id="logo">
                                  <div id="logo_text">
                                        <h1><a href="app.php">Inter<span
class="logo_colour">operabilidad</span></a></h1>
                                        <h2>Interoperabilidad y compartici&oacute;n
de recursos entre dominios Active Directory y servidores Linux</h2>
                                        <h2><noscript><img id="alert"
src="style/warning.png">Para un correcto funcionamiento de la aplicaci&oacute;n habilitar
javascript en su navegador!</noscript></h2>
                                        <?php
                                              if(!$_SESSION['root_group']){
                                                    echo "<h2><img id=\"alert\"
src=\"style/warning.png\">El usuario no esta habilitado para realizar configuraciones en el
sistema!</h2>";
                                        }
```

```
                                        ?>
                                    </div>
                                </div>
                                <div id="menubar">
                                    <ul id="menu">
                                        <li><a href="Host.php">HOST</a></li>
                                        <li><a
href="Autenticar.php">AUTENTICACI&Oacute;N</a></li>
                                        <li><a
href="Integrar.php">INTEGRACI&Oacute;N</a></li>
                                        <li><a
href="Info.php">INFORMACI&Oacute;N</a></li>
                                        <li><a
href="Servidores.php">SERVIDORES</a></li>
                                    </ul>
                                </div>
                            </div>
                            <div id="site_content">
                                <div id="content_info">
                                    <?php
                                        echo "<h2>Servidores Enlazados:</h2>";
                                        $db=conecta_db('functions/Integracion.db');
                                        $result=$db->query('select id, nombre, ip,
winbind_domain, ads_realm, dc_server, krb_domain, krb_dc_server, ads_info, estado from host');
                                        $i=1;
                                        foreach($result as $row){
                                            echo "<table id=\"t".$i."\"
class=\"servers\" name=\"t".$i."\">";
                                            echo "<caption>Nombre:
".$row['nombre']."</caption>";
                                            echo "<tbody>";
                                            echo
"<tr><td>IP</th><td>".$row['ip']."</td></tr>";
                                            echo
"<tr><td>Enlazado</th><td>SI</td></tr>";
                                            echo "<tr><td class=\"info_td\"
colspan=\"2\">Informacion del Dominio</td></tr>";
                                            $info_domain= explode("\n",
$row['ads_info']);
                                            foreach($info_domain as $info){
                                                if($info_domain!='\n'){
                                                    $var =
explode(":",$info);
                                                    echo
"<tr><td>".$var[0]."</td><td>".$var[1]."</td></tr>";
                                                }
                                            }
                                            echo "<tr><td class=\"info_td\"
colspan=\"2\">Configuraci&oacute;n de integraci&oacute;n</td></tr>";
                                            echo "<tr><td>Dominio
Winbind</d><td>".$row['winbind_domain']."</td></tr>";
```

```
                                                        echo "<tr><td>ADS
realm</td><td>".$row['ads_realm']."</td></tr>";
                                                        echo "<tr><td>Comtrolador de
domino</td><td>".$row['dc_server']."</td></tr>";
                                                        echo "<tr><td class=\"info_td\"
colspan=\"2\">Configuraci&oacute;n de auntentica&oacute;n</td></tr>";
                                                        echo
"<tr><td>Dominio</td><td>".$row['krb_domain']."</td></tr>";
                                                        echo "<tr><td>Controlador de
dominio</td><td>".$row['krb_dc_server']."</td></tr>";
                                                        echo "<tr><td class=\"info_td\"
colspan=\"2\">NTP</td></tr>";
                                                        $ntp=$db->query('select ntp_server
from ntp where host_id='.$row['id'].' and estado=1');
                                                        foreach($ntp as $server){
                                                                echo "<tr><td
colspan=\"2\">".$server['ntp_server']."</td></tr>";
                                                        }
                                                        echo "<tr><td class=\"info_td\"
colspan=\"2\">DNS</td></tr>";
                                                        $dns=$db->query('select dns_server
from dns where host_id='.$row['id'].' and estado=1');
                                                        foreach($dns as $server){
                                                                echo "<tr><td
colspan=\"2\">".$server['dns_server']."</td></tr>";
                                                        }
                                                        echo "</tbody>";
                                                        echo "</table>";
                                                        $i++;
                                                }
                                                echo "<p id=\"pie_servers\">";
                                                for($j=1 ; $j<$i ; $j++){
                                                        echo "<a href=\"#t".$j."\"
onClick=\"table_servers('t".$j."');\" > ".$j." </a>";
                                                }
                                                echo"</p>";
                                                $db=null;
                                        ?>
                                </div>
                        </div>
                        <div id="footer">
                                Proyecto de grado de Lic. en Redes y Sistemas Operativos | <a
href=\"http://espol.edu.ec\" target="_blank">ESPOL</a>
                        </div>
                </div>
                <?php
                        if($_GET['error']){
                                echo "<div class=\"mensaje_main\">";
                                echo "<div class=\"mensaje\">";
                        }
                        if($_GET['error']=="pak1"){
```

```
                                        echo "<h2 class=\"error\">NO se pudo instalar el
paquete</h2>";
                                }
                                if($_GET['error']){
                                        echo "<div id=\"div_button\">";
                                        echo "<a id=\"button\" href=\"Info.php\">Aceptar</a>";
                                        echo "</div>";
                                        echo "</div>";
                                        echo "</div>";
                                }
                        ?>
        </body>
</html>
```

Authconfig.php

Funcion que integra el sistema Linux al dominio.

```
<?php
  include 'coneccion.php';
        include 'validar.php';
        session_start();
        if($_POST['wdc']!="" && $_POST['wd']!="" && $_POST['war']!="" && $_POST['adm']!=""
&& $_POST['password_adm']!=""){
                if(validar_nombre($_POST['wdc']) && validar_nombre($_POST['wd']) &&
validar_nombre($_POST['war'])){
                                $var=ejecutar('ll /etc/samba/ | grep "smb.conf.bak"');
                                if($var['out']==""){
                                        ejecutar('cat /etc/samba/smb.conf >
/etc/samba/smb.conf.bak');
                                }
                                $var=ejecutar('grep "idmap config" /etc/samba/smb.conf');
                                if($var['out']!=""){
                                        ejecutar('sed -i".old" \'/:backend/c idmap config
'.$_POST['wd'].':backend = rid\' /etc/samba/smb.conf');
                                        ejecutar('sed -i".old" \'/:base_rid/c idmap config
'.$_POST['wd'].':base_rid = 0\' /etc/samba/smb.conf');
                                        ejecutar('sed -i".old" \'/:range/c idmap config
'.$_POST['wd'].':range = 100000 - 199999\' /etc/samba/smb.conf');
                                }else{
                                        $pos=ejecutar('grep -Hn \'global]\' /etc/samba/smb.conf | cut
-d\':\' -f2');
                                        $line=intval($pos['out']);
                                        ejecutar('sed -i".old" \''.$line.'a idmap config
'.$_POST['wd'].':range = 100000 - 199999\' /etc/samba/smb.conf');
                                        ejecutar('sed -i".old" \''.$line.'a idmap config
'.$_POST['wd'].':base_rid = 0\' /etc/samba/smb.conf');
                                        ejecutar('sed -i".old" \''.$line.'a idmap config
'.$_POST['wd'].':backend = rid\' /etc/samba/smb.conf');
                                }
```

```
                        $comando="authconfig  --update --enablewinbind --enablewinbindauth
--smbsecurity=ads --smbworkgroup=".$_POST['wd']." --smbrealm=".$_POST['war']." --
smbservers=".$_POST['wdc']." --smbidmapuid=10000-19999  --smbidmapgid=10000-19999 --
winbindjoin=".$_POST['adm']."%'".$_POST['password_adm']."' --
winbindtemplatehomedir=/home/%D/%U --winbindseparator=+ --
winbindtemplateshell=/bin/bash --enablewinbindusedefaultdomain --enablemkhomedir --
enablelocauthorize";
                        ejecutar($comando);
                        $var=ejecutar("net join -S ".$_POST['wdc']."  -U
".$_POST['adm']."%'".$_POST['password_adm']."' | grep \"Joined '\"");
                        if($var['out']!=""){
                                $_SESSION['enlazado']=TRUE;
                                $var=ejecutar('net ads info | sed \'/Server/d\'');
                                $_SESSION['ads_info']=$var['out'];
                                ejecutar('service smb restart');
                                header ('Location: ../Integrar.php?error=auth_yes');
                        }else{
                                $_SESSION['ads_info']="";
                                if($_SESSION['enlazado']){
                                        $_SESSION['enlazado']=FALSE;
                                        header ('Location: ../Integrar.php?error=auth2');
                                }else{
                                        $_SESSION['enlazado']=FALSE;
                                        header ('Location: ../Integrar.php?error=auth1');
                                }
                        }
                }else{
                        header ('Location: ../Integrar.php?error=auth0');
                }
        }else{
                header ('Location: ../Integrar.php?error=auth0');
        }
?>
```

Coneccion.php

Archivo con las funciones de coneccion y ejecución de comando del sistema Linux.

```
<?php
  function coneccion(){
     session_start();
     $connection = ssh2_connect($_SESSION['servidor'], 22);
     $usuario = $_SESSION['usuario'];
     $password = $_SESSION['password'];
     ssh2_auth_password($connection, $usuario, $password);
     return $connection;
  }
  function ejecutar($comando){
     $stream = ssh2_exec(coneccion(), $comando);
     stream_set_blocking($stream, true);
```

```
    $error_stream = ssh2_fetch_stream($stream, SSH2_STREAM_STDERR);
    stream_set_blocking($error_stream, true);
    $stream_out = ssh2_fetch_stream($stream, SSH2_STREAM_STDIO);
    $out=stream_get_contents($stream_out);
    $error = stream_get_contents($error_stream);
    $var = array(
      "out"   =>  $out,
      "error" =>  $error);
    return $var;
  }
?>
```

Dns.php

Funcion que agrega el DNS al sistema Linux.

```
<?php
  include 'coneccion.php';
        include 'validar.php';
        if($_POST['dnsserver']!=""){
                if(validar_ip4($server)){
                        ejecutar('sed -i".old" \'$a nameserver '.$_POST['dnsserver'].'\'
/etc/resolv.conf');
                        $var=ejecutar('grep -w '.$_POST['dnsserver'].' /etc/resolv.conf');
                        if($var['out']){
                                header ('Location: ../Host.php');
                        }else{
                                header ('Location: ../Host.php?error=dns1');
                        }
                }else{
                        header ('Location: ../Host.php?error=dns0');
                }
        }else{
                header ('Location: ../Host.php?error=dns0');
        }
?>
```

Elininar_dns.php

Función que elimina un DNS del sistema Linux.

```
<?php
  include 'coneccion.php';
        include 'funciones_db.php';
  ejecutar("sed -i\".old\" 's/\<nameserver ".$_GET['dnsserver']."\>//g' /etc/resolv.conf");
  $var=ejecutar('grep -w '.$_GET['dnsserver'].' /etc/resolv.conf');
  if($var['out']==""){
                dns_remove_db('Integracion.db',$_GET['dnsserver']);
```

```
                    header ('Location: ../Host.php');
  }else{
    header ('Location: ../Host.php?error=dns2');
  }
?>
```

Elininar_kerberos.php

Funcion que erestaura la configuración por defecto de Kerberos.

```
<?php
include 'coneccion.php';
$conf='[logging]
  default = FILE:/var/log/krb5libs.log
  kdc = FILE:/var/log/krb5kdc.log
  admin_server = FILE:/var/log/kadmind.log

[libdefaults]
  default_realm = example.com
  dns_lookup_realm = false
  dns_lookup_kdc = false
  ticket_lifetime = 24h
  renew_lifetime = 7d
  forwardable = true

[realms]
  example.com = {
  kdc = kerberos.example.com
  admin_server = kerberos.example.com
  }

[domain_realm]
  .demo = example.com
  demo = example.com';
  ejecutar('echo -e "'.$conf.'" > /etc/krb5.conf');
        $var=ejecutar('grep  example.com  /etc/krb5.conf');
  if($var['out']!=""){
    header ('Location: ../Autenticar.php');
  }else{
    header ('Location: ../Autenticar.php?error_eli_krb=a');
  }
?>
```

Eliminar_ntp.php

Funcion que elimina un servidor NTP del sistema.

```
<?php
```

```
   include 'coneccion.php';
            include 'funciones_db.php';
   ejecutar('sed -i".old" \'s/\<server '.$_GET['server'].'\>//g\' /etc/ntp.conf');
   $var=ejecutar('grep -w '.$_GET['server'].' /etc/ntp.conf');
   if($var['out']==""){
                        ntp_remove_db('Integracion.db',$_GET['server']);
                        header ('Location: ../Host.php');
   }else{
     header ('Location: ../Host.php?error=ntp5');
   }
?>
```

Funciones_db.php

Funciones que se emplean para agregar datos a la base.

```
<?php
function conecta_db($file_db){
   try {
      $db = new PDO('sqlite:'.$file_db);
      return($db);
   } catch (PDOException $e) {
      print "<p>Error: No puede conectarse con la base de datos.</p>\n";
      exit();
   }
}


function crear_db($file_db){
            $db=conecta_db($file_db);
            $sql ='CREATE TABLE IF NOT EXISTS "dns" ("id" INTEGER PRIMARY KEY  NOT NULL
,"dns_server" TEXT, "host_id" INTEGER,"estado" INTEGER)';
            $db->query($sql);
            $sql ='CREATE TABLE IF NOT EXISTS "host" ("id" INTEGER PRIMARY KEY  NOT NULL
,"nombre" TEXT,"ip" TEXT,"winbind_domain" TEXT,"ads_realm" TEXT, "dc_server"
TEXT,"krb_domain" TEXT, "krb_dc_server" TEXT,  "ads_info" TEXT, "estado" INTEGER)';
            $db->query($sql);
            $sql='CREATE TABLE IF NOT EXISTS "ntp" ("id" INTEGER PRIMARY KEY  NOT NULL ,
"ntp_server" TEXT, "host_id" INTEGER,"estado" INTEGER)';
            $db->query($sql);
            $db=null;
            return;
}

function host_db($file_db){
            session_start();
            $db=conecta_db($file_db);
            $sql='select count(id) as ID  from host where nombre=\''.$_SESSION['hostname'].'\'';
            $result=$db->query($sql);
            $estado=0;
```

```
		if($_SESSION['enlazado']){
			$estado=1;
		}
		foreach($result as $row){
			$count=$row['ID'];
		}
		if($count==0){
			$sql='insert into host (id,nombre,ip,ads_info,estado) values ((select count(id)+1
from host),\''.$_SESSION['hostname']
.'\',\''.$_SESSION['ip'].'\',\''.$_SESSION['ads_info'].'\','.$estado.')';
			$db->query($sql);
		}else{
			$sql='update host set nombre=\''.$_SESSION['hostname'] .'\',
ip=\''.$_SESSION['ip'].'\', ads_info=\''.$_SESSION['ads_info'].'\', estado='.$estado.' where
id=(select id  from host where nombre="'.$_SESSION['hostname'].'")';
			$db->query($sql);
		}
		$sql='select id  from host where nombre="'.$_SESSION['hostname'].'"';
		$result=$db->query($sql);
		foreach($result as $row){
			$id=$row['id'];
		}
		$_SESSION['id_host']=$id;
		$db=null;
		return;

}

function cambiar_host($file_db){
		session_start();
		$db=conecta_db($file_db);
		$sql='update host set nombre=\''.$_SESSION['hostname'] .'\' where
id='.$_SESSION['id_host'];
		$db->query($sql);
		$db=null;
		return;
}

function ntp_db($file_db,$server){
		session_start();
		$db=conecta_db($file_db);
		$sql='select count(id) as ID from ntp where host_id='.$_SESSION['id_host'].' and
ntp_server="'.$server.'"';
		$result=$db->query($sql);
		foreach($result as $row){
			$count=$row['ID'];
		}
		if($count==0){
			$sql='insert into ntp (id, ntp_server, host_id, estado) values((select count(id)+1
from ntp),\''.$server.'\','.$_SESSION['id_host'].',1)';
			$db->query($sql);
```

```
		}else{
			$sql='update ntp set estado=1 where id=(select id from ntp where
host_id='.$_SESSION['id_host'].' and ntp_server="'.$server.'")';
			$db->query($sql);
		}
		$db=null;
		return;
}

function dns_db($file_db,$server){
		session_start();
		$db=conecta_db($file_db);
		$sql='select count(id) as ID from dns where host_id='.$_SESSION['id_host'].' and
dns_server="'.$server.'"';
		$result=$db->query($sql);
		foreach($result as $row){
		$count=$row['ID'];
		}
		if($count==0){
			$sql='insert into dns (id, dns_server, host_id, estado) values((select count(id)+1
from dns),\''.$server.'\','.$_SESSION['id_host'].',1)';
			$db->query($sql);
		}else{
			$sql='update dns set estado=1 where id=(select id from dns where
host_id='.$_SESSION['id_host'].' and dns_server="'.$server.'")';
			$db->query($sql);
		}
		$db=null;
		return;
}

function krb_db($file_db, $domain, $dc){
		session_start();
		$db=conecta_db($file_db);
		$sql='update host set krb_domain=\''.$domain.'\', krb_dc_server=\''.$dc.'\' where
id='.$_SESSION['id_host'];
		$db->query($sql);
		$db=null;
		return;
}

function sw_db($file_db, $domain, $ads, $dc){
		session_start();
		$estado=0;
		if($_SESSION['enlazado']){
			$estado=1;
		}
		$db=conecta_db($file_db);
		$sql='update host set winbind_domain=\''.$domain.'\', ads_realm=\''.$ads.'\',
dc_server=\''.$dc.'\', ads_info=\''.$_SESSION['ads_info'].'\', estado='.$estado.' where
id='.$_SESSION['id_host'];
```

```
	$db->query($sql);
	$db=null;
	return;
}

function ntp_remove_db($file_db,$server){
	session_start();
	$db=conecta_db($file_db);
	$sql='update ntp set estado=0 where id=(select id from ntp where
host_id='.$_SESSION['id_host'].' and ntp_server="'.$server.'")';
	$db->query($sql);
	$db=null;
	return;
}

function dns_remove_db($file_db,$server){
	session_start();
	$db=conecta_db($file_db);
	$sql='update dns set estado=0 where id=(select id from dns where
host_id='.$_SESSION['id_host'].' and dns_server="'.$server.'")';
	$db->query($sql);
	$db=null;
	return;
}

?>
```

Hostname.php

Funcion que cambia Hostname del sitema.

```
<?php
	include 'coneccion.php';
	include 'validar.php';
	if($_POST['nombre']!=""){
		if(validar_nombre($_POST['nombre'])){
			session_start();
			$host=explode(".",$_POST['nombre']);
			ejecutar('sed -i".old" \'/HOSTNAME/d\' /etc/sysconfig/network');
			ejecutar('echo \'HOSTNAME='.$_POST['nombre'].'\' >>
/etc/sysconfig/network ');
			$var=ejecutar('grep '.$_POST['nombre'].' /etc/sysconfig/network');
			if($var['out']!=""){
				cambiar_host('Integracion_db');
				ejecutar('init 6');
				session_destroy();
				header('location: ../index.php');
			}else{
				header('location: ../Host.php?error=host1');
			}
```

```
                }else{
                        header('location: ../Host.php?error=host0');
                }
        }else{
                header('location: ../Host.php?error=host0');
        }
?>
```

Instalar.php

Funcion que instala paquetes faltantes.

```
<?php
        include_once  'coneccion.php';
        session_start();

        function paquetes(){
                session_start();
                $var1 = ejecutar('rpm -q samba > paq.txt | cat paq.txt | grep \'is not\'');
                $var2 = ejecutar('rpm -q samba-common >> paq.txt | cat paq.txt | grep \'is
not\'');
                $var3 = ejecutar('rpm -q samba-client >> paq.txt | cat paq.txt | grep \'is not\'');
                $var4 = ejecutar('rpm -q samba-winbind >> paq.txt | cat paq.txt | grep \'is
not\'');
                $var5 = ejecutar('rpm -q samba-winbind-clients >> paq.txt | cat paq.txt | grep
\'is not\'');
                $var6 = ejecutar('rpm -q krb5-workstation >> paq.txt | cat paq.txt | grep \'is
not\'');
                $var7 = ejecutar('rpm -q oddjob-mkhomedir >> paq.txt | cat paq.txt | grep \'is
not\'');
                $var = ejecutar('cat paq.txt');
                $_SESSION['paquetes'] = explode("\n",$var['out']);
                if ($var1['out']=="" && $var2['out']=="" && $var3['out']=="" &&
$var4['out']=="" &&$var5['out']=="" && $var6['out']=="" && $var7['out']==""){
                        $_SESSION['requisitos']=TRUE;
                        return;
                }else{
                        $_SESSION['requisitos']=FALSE;
                }
        }

        $url="http://".$_SERVER['HTTP_HOST'].":".$_SERVER['SERVER_PORT'].$_SERVER['PHP_
SELF'];
        $archivo = str_replace('instalar.php', 'packages/', $url);

        if($_SESSION['arquitectura']=="x86_64"){
                switch ($_GET['paquete']){
                        case 0:
                                ejecutar('wget '.$archivo.'samba-3.5.4-68.el6.x86_64.rpm');
                                ejecutar('rpm -i samba-3.5.4-68.el6.x86_64.rpm');
```

```
                                        break;
                                case 1:
                                        ejecutar('wget '.$archivo.'samba-common-3.5.4-
68.el6.x86_64.rpm');
                                        ejecutar('rpm -i samba-common-3.5.4-68.el6.x86_64.rpm');
                                        break;
                                case 2:
                                        ejecutar('wget '.$archivo.'samba-client-3.5.4-
68.el6.x86_64.rpm');
                                        ejecutar('rpm -i samba-client-3.5.4-68.el6.x86_64.rpm');
                                        break;
                                case 3:
                                        ejecutar('wget '.$archivo.'samba-winbind-3.5.4-
68.el6.x86_64.rpm');
                                        ejecutar('rpm -i samba-winbind-3.5.4-68.el6.x86_64.rpm');
                                        break;
                                case 4:
                                        ejecutar('wget '.$archivo.'samba-winbind-clients-3.5.4-
68.el6.x86_64.rpm');
                                        ejecutar('rpm -i samba-winbind-clients-3.5.4-
68.el6.x86_64.rpm');
                                        break;
                                case 5:
                                        ejecutar('wget '.$archivo.'krb5-workstation-1.8.2-
3.el6.x86_64.rpm');
                                        ejecutar('rpm -i krb5-workstation-1.8.2-3.el6.x86_64.rpm');
                                        break;
                                case 6:
                                        ejecutar('wget '.$archivo.'oddjob-mkhomedir-0.30-
1.el6.x86_64.rpm');
                                        ejecutar('rpm -i oddjob-mkhomedir-0.30-1.el6.x86_64.rpm');
                                        break;
                                default:
                                        break;
                        }
                        paquetes();
                        header ('Location: ../Info.php');
                }else{
                        if($_SESSION['arquitectura']=="i686"){
                        switch ($_GET['paquete']){
                                case 0:
                                        ejecutar('wget '.$archivo.'samba-3.5.4-68.el6.i686.rpm');
                                        ejecutar('rpm -i samba-3.5.4-68.el6.i686.rpm');
                                        break;
                                case 1:
                                        ejecutar('wget '.$archivo.'samba-common-3.5.4-
68.el6.i686.rpm');
                                        ejecutar('rpm -i samba-common-3.5.4-68.el6.i686.rpm');
                                        break;
                                case 2:
                                        ejecutar('wget '.$archivo.'samba-client-3.5.4-68.el6.i686.rpm');
```

```
                                        ejecutar('rpm -i samba-client-3.5.4-68.el6.i686.rpm');
                                        break;
                                case 3:
                                        ejecutar('wget '.$archivo.'samba-winbind-3.5.4-
68.el6.i686.rpm');
                                        ejecutar('rpm -i samba-winbind-3.5.4-68.el6.i686.rpm');
                                        break;
                                case 4:
                                        ejecutar('wget '.$archivo.'samba-winbind-clients-3.5.4-
68.el6.i686.rpm');
                                        ejecutar('rpm -i samba-winbind-clients-3.5.4-
68.el6.i686.rpm');
                                        break;
                                case 5:
                                        ejecutar('wget '.$archivo.'krb5-workstation-1.8.2-
3.el6.i686.rpm');
                                        ejecutar('rpm -i krb5-workstation-1.8.2-3.el6.i686.rpm');
                                        break;
                                case 6:
                                        ejecutar('wget '.$archivo.'oddjob-mkhomedir-0.30-
1.el6.i686.rpm');
                                        ejecutar('rpm -i oddjob-mkhomedir-0.30-1.el6.i686.rpm');
                                        break;
                                default:
                                        break;
                        }
                        paquetes();
                        echo $archivo.'samba-client-3.5.4-68.el6.i686.rpm';
                        header ('Location: ../Info.php');
                        }else{
                                header ('Location: ../Info.php?error=pak1');
                        }
        }
?>
```

Kerberos.php

Funcion que configura el cliente Kerberos.

```
<?php
include 'coneccion.php';
include 'funciones_db.php';
include 'validar.php';
if($_POST['domain']!="" && $_POST['dc']!=""){
if(validar_nombre($_POST['domain']) && validar_nombre($_POST['dc'])){
        $dominio=strtoupper($_POST['domain']);
        $dc=strtoupper($_POST['dc']);
        $conf='[logging]
  default = FILE:/var/log/krb5libs.log
  kdc = FILE:/var/log/krb5kdc.log
```

```
   admin_server = FILE:/var/log/kadmind.log

[libdefaults]
   default_realm = '.$dominio.'
   dns_lookup_realm = false
   dns_lookup_kdc = false
   ticket_lifetime = 24h
   renew_lifetime = 7d
   forwardable = true

[realms]
   '.$dominio.' = {
   kdc = '.$dc.'
   admin_server = '.$dc.'
   }

[domain_realm]
   .demo = '.$dominio.'
   demo = '.$dominio;
   ejecutar('echo -e "'.$conf.'" > /etc/krb5.conf ');
         $var=ejecutar('grep -w '.$dominio.' /etc/krb5.conf');
   if($var['out']!=""){
      ejecutar('sed -i".old" \'/search/d\' /etc/resolv.conf');
      ejecutar('sed -i".old" \'/domain/d\' /etc/resolv.conf');
                  ejecutar('sed -i".old" \'1a domain '.$dominio.'\' /etc/resolv.conf');
                  ejecutar('sed -i".old" \'1a search '.$dominio.'\' /etc/resolv.conf');
                  $var=ejecutar('grep -w '.$dominio.' /etc/resolv.conf');
                  if($var['out']!=""){
         session_start();
         $wd = explode(".",$dominio);
         $_SESSION['wd']=$wd[0];
         $_SESSION['war']=$dominio;
         $_SESSION['wdc']=$dc;
         $_SESSION['dominio']=TRUE;
                              krb_db('Integracion.db', $dominio, $dc);
                              header ('Location: ../Integrar.php?error=dk_yes');
      }else{
         header ('Location: ../Autenticar.php?error=krb2');
      }
   }else{
      header ('Location: ../Autenticar.php?error=krb1');
   }
         }else{
                  header ('Location: ../Autenticar.php?error=krb0');
         }
}else{
         header ('Location: ../Autenticar.php?error=krb0');
}
?>
```

Logout.php

Funcion para salir de la herramienta.

```
<?php
   //Crear sesión
   session_start();
   //Destruir Sesión
   session_destroy();
   //Redireccionar a login.php
   header('location: ../index.php');
?>
```

Monitoreo.php

Funcion que ejecuta los comandos de monitoreo para la herramienta.

```
<?php
include 'coneccion.php';
$var=ejecutar("smbstatus -S | sed '/\-/d' && smbstatus -L | sed '/\-/d' | sed '/Locked/d'");
$lines = explode("\n", $var['out']);
            echo "<h2>Recursos compartidos por el servidor:</h2>";
            echo "<table><tbody>";
            $col='colspan="2"';
            $i=TRUE;
            $j=TRUE;
                        foreach($lines as $line){
                                    echo "<tr>";
                                    $tds=explode("  ", $line);
                                    foreach($tds as $td){
                                                if($td=='Service' || $td==' Connected at' || $td=='Pid' ||
$td=='Group' || $td==' machine' || $td=='pid' || $td=='Uid' || $td=='DenyMode' || $td==' Access' ||
$td=='R/W' || $td=='Oplock' || $td==' SharePath' || $td==' Name' || $td==' Time'){
                                                            switch ($td) {
                                                                        case 'Service':
                                                                                    echo "<th colspan=3
>Servicio</th>";
                                                                                    break;
                                                                        case 'Username':
                                                                                    echo "<th>Usuario</th>";
                                                                                    break;
                                                                        case 'Group':
                                                                                    echo "<th>Grupo</th>";
                                                                                    break;
                                                                        case ' machine':
                                                                                    echo "<th
".$col.">Maquina</th>";
                                                                                    break;
                                                                        case ' Access':
                                                                                    echo "<th>Acceso</th>";
```

```
                                                                        break;
                                                                case ' SharePath':
                                                                        echo "<th>Ruta</th>";
                                                                        break;
                                                                case ' Name':
                                                                        echo
"<th>Archivo/Directorio</th>";
                                                                        break;
                                                                case ' Time':
                                                                        echo "<th>Tiempo</th>";
                                                                        break;
                                                                case ' Connected at':
                                                                        echo "<th ".$col.">Fecha de
conecci&oacute;n</th>";
                                                                        break;
                                                                case 'Pid':
                                                                        $col='';
                                                                        $j=FALSE;
                                                                        echo "<th>".$td."</th>";
                                                                        break;
                                                                default:
                                                                        echo "<th ".$col.">".$td."</th>";
                                                                        break;
                                                        }
                                                }else{
                                                        if($td!=""){
                                                                if($td=='No locked files'){
                                                                        echo "<td colspan=9 >No hay
conecciones</td>";
                                                                }else{
                                                                        if($i){
                                                                                        echo "<td
colspan=3 >".$td."</td>";
                                                                        }else{
                                                                                echo "<td
".$col.">".$td."</td>";
                                                                        }
                                                                }
                                                        }
                                                        $i=FALSE;
                                                }
                                                echo "</tr>";
                                                $i=$j;
                        }
        echo "</table></tbody>";
?>
```

Ntp.php

Funicon que agrega un servidor dns al sistema.

```
<?php
	include 'coneccion.php';
	$server=$_POST['ipserver'];
	if($server!=""){
		$var=ejecutar('service ntpd stop | grep -E "OK|FAILED"');
		if ($var['out']!="") {
			$var=ejecutar('ntpdate '.$server.' | grep \'no server\'');
			if($var['error']=="") {
				$var=ejecutar('grep -w "server '.$server.'" /etc/ntp.conf');
				if($var['out']==""){
					ejecutar('sed -i".old" \'$a server '.$server.'\'
/etc/ntp.conf');
					$var=ejecutar('grep   "server '.$server.'"
/etc/ntp.conf');
					if($var['out']!=""){
						$var=ejecutar('service ntpd start | grep -E
"OK|Starting"');
						if ($var['out']!=""){
							header ('Location:
../Host.php?error=ntp_yes');
						}else{
							header ('Location:
../Host.php?error=ntp4');
						}
					}else {
						header ('Location: ../Host.php?error=ntp3');
					}
				}else{
					header ('Location: ../Host.php?error=ntp_yes');
				}
			}else {
				header ('Location: ../Host.php?error=ntp2');
			}
		}else {
			header ('Location: ../Host.php?error=ntp1');
		}
	}else{
		header ('Location: ../Host.php?error=ntp0');
	}
?>
```

Servers.php

Funcion que muestra la información de la base de datos.

```
<?php
	include 'coneccion.php';
```

```
	function servers_ntp(){
		$comando='grep ^server /etc/ntp.conf | awk \'{ print $2 }\'';
		$var=ejecutar($comando);
		$servers = explode("\n", $var['out']);
		return $servers;
	}

	function servers_dns(){
		$comando='grep ^nameserver /etc/resolv.conf | awk \'{ print $2 }\'';
		$var=ejecutar($comando);
		$servers = explode("\n", $var['out']);
		return $servers;
	}

	function domain(){
				$comando='cat /etc/krb5.conf | grep default_realm | awk \'{ print $3
}\'';
				$var1=ejecutar($comando);
				$comando='cat /etc/krb5.conf | grep "kdc = " | awk \'{ print $3 }\'';
				$dc=ejecutar($comando);
				$var2=explode("\n",$dc['out']);
				$var=array($var1['out'],$var2[2]);
				return $var;
	}

	function dominio_winbind(){
				session_start();
				$comando='grep -w "workgroup =" /etc/samba/smb.conf | sed \'/;/d\'
| sed \'/#/d\' | grep "workgroup =" | awk \'{ print $3}\'';
				$wd=ejecutar($comando);
				$comando='grep -w "password server =" /etc/samba/smb.conf | sed
\'/;/d\' | sed \'/#/d\' | grep "password server =" | awk \'{ print $4}\'';
				$wdc=ejecutar($comando);
				$comando='grep   -w "realm =" /etc/samba/smb.conf | sed \'/;/d\' |
sed \'/#/d\' | grep "realm =" | awk \'{ print $3}\'';
				$war=ejecutar($comando);
				$var=array(
				"wd" => $wd['out'],
				"wdc" =>$wdc['out'],
				"war" =>$war['out']);
				return $var;
	}

	function paquetes(){
		session_start();
		$var1 = ejecutar('rpm -q samba > paq.txt | cat paq.txt | grep \'is not\'');
		$var2 = ejecutar('rpm -q samba-common >> paq.txt | cat paq.txt | grep \'is
not\'');
		$var3 = ejecutar('rpm -q samba-client >> paq.txt | cat paq.txt | grep \'is not\'');
		$var4 = ejecutar('rpm -q samba-winbind >> paq.txt | cat paq.txt | grep \'is
not\'');
```

```
		$var5 = ejecutar('rpm -q samba-winbind-clients >> paq.txt | cat paq.txt | grep
\'is not\'');
		$var6 = ejecutar('rpm -q krb5-workstation >> paq.txt | cat paq.txt | grep \'is
not\'');
		$var7 = ejecutar('rpm -q oddjob-mkhomedir >> paq.txt | cat paq.txt | grep \'is
not\'');
		$var = ejecutar('cat paq.txt');
		$_SESSION['paquetes'] = explode("\n",$var['out']);
		if ($var1['out']=="" && $var2['out']=="" && $var3['out']=="" &&
$var4['out']=="" &&$var5['out']=="" && $var6['out']=="" && $var7['out']==""){
			$_SESSION['requisitos']=TRUE;
			return;
		}else{
			$_SESSION['requisitos']=FALSE;
			header ('Location: ../Info.php');
		}
	}

	function data_host(){
		session_start();
		$var=ejecutar('groups | grep -w \'root\'');
		if($var['out']){
			$_SESSION['root_group']=TRUE;
			$var = ejecutar('ifconfig | grep \'inet addr:\' | awk \'{print $2}\' | cut -
d\':\' -f2');
			$ip = explode("\n",$var['out']);
			$_SESSION['ip'] = $ip[0];
			$var = ejecutar('hostname');
			$_SESSION['hostname'] = $var['out'];
			$var=ejecutar('groups | grep -w \'root\'');
			if($var['out']){
				$_SESSION['root_group']=TRUE;
			}
			$var=ejecutar('net ads testjoin | grep "Join is OK"');
			if($var['out']!=""){
				$var=ejecutar('net ads info | sed \'/Server/d\'');
				$_SESSION['enlazado']=TRUE;
				if($var['out']!=""){
					$_SESSION['ads_info']=$var['out'];
				}
			}
			$var = ejecutar('uname --all | grep "x86_64"');
			if($var['out']){
				$_SESSION['arquitectura']="x86_64";
			}else{
				$var = ejecutar('uname --all | grep "i686"');
				if($var['out']){
					$_SESSION['arquitectura']="i686";
					return true;
				}
			}
```

```
                return true;
        }else{
                $var = ejecutar('hostname');
                $_SESSION['hostname'] = $var['out'];
                return false;
        }
    }

?>
```

Sincornizar_ntp.php

Funcion que sincroniza el reloj del sistema con el del servidor NTP.

```
<?php
  include 'coneccion.php';
        $var=ejecutar('service ntpd stop | grep -E "OK|FAILED"');
  if ($var['out']!=""){
        $var=ejecutar('ntpdate '.$_GET['server'].' | grep "no server"');
    if ($var['error']=="") {
                $var=ejecutar('service ntpd start | grep -E "OK|Starting"');
      if ($var['out']!=""){
            header ('Location: ../Host.php?error=ntp_yes');
      }else{
                        header ('Location: ../Host.php?error=ntp4');
      }
    }else{
                $var=ejecutar('service ntpd start | grep -E "OK|Starting"');
    }
  }else{
    header ('Location: ../Host.php?error=ntp1');
  }
?>
```

Validar.php

Funciones que validadn nombre de dominio y dirección IP.

```
<?php
        function validar_nombre($nombre){

        $permitidos='abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ012345
6789-_.';
                for ($i=0; $i<strlen($nombre); $i++){
                        if (strpos($permitidos, substr($nombre,$i,1))===false){
                                return false;
                        }
                }
                return true;
```

```
	}

	function validar_ip4($ip){
		if(filter_var($ip, FILTER_VALIDATE_IP)){
			return true;
		}else{
			return false;
		}
	}
?>
```

Validar_usuario.php

Funcion que autentica al ususario y recopila información del sistema.

```
<?php
include 'servers.php';
include 'funciones_db.php';
if($_POST['servidor']!="" && $_POST['admin']!="" && $_POST['password_usuario']!="" ){
$servidor=$_POST['servidor'];
$connection = ssh2_connect($servidor, 22);
$usuario = $_POST['admin'];
$password = $_POST['password_usuario'];
if (ssh2_auth_password($connection, $usuario, $password)) {
session_start();
$_SESSION['autenticado'] = TRUE;
$_SESSION['usuario'] = $usuario;
$_SESSION['password'] = $password;
$_SESSION['servidor'] = $servidor;
$_SESSION['dominio']=FALSE;
crear_db('Integracion.db');
if(data_host()){
host_db('Integracion.db');
}
paquetes();
header('Location: ../Host.php');
} else {
header('Location: ../index.php?error_login=yes');
}
}else{
header('Location: ../index.php?error_login=yes');
}
?>
```

BIBLIOGRAFÍA

1. ISO/IEC 27001 Seguridad de la información.(s.f.). Recuperado el 18/02/2010, de http://www.bsigroup.es/es/certificacion-y-auditoria/Sistemas-de-gestion/estandares-esquemas/ISOIEC-27001
2. ISO/IEC 27001:2005.(s.f.). Recuperado el 18/02/2010, de http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=42103
3. La serie 27000. (s.f.). Recuperado el 18/02/2010, de http://www.iso27000.es/iso27000.html
4. Barboza Fabian, Diseñando una infraestructura de red con active directory, Capítulos 2,3,4.
5. Mark Heslin. Integrating Red Hat Enterprise Linux 6 with Active Directory. Red Hat Enterprise. Febrero 2013
6. Lerdorf R, Tatroe K y MacIntyre P. Programming Php. O'Reilly. Febrero 2012

7. Winbind authentication against active directory. http://wiki.centos.org/TipsAndTricks/WinbindADS
8. Samba's idmap_rid Backend for Winbind. http://www.samba.org/samba/docs/man/manpages-3/idmap_rid.8.html
9. Secure Shell2. http://www.php.net/manual/en/book.ssh2.php
10. Server Security (User Level Security). http://www.samba.org/samba/docs/man/Samba-HOWTO-Collection/ServerType.html#id2560266
11. Manual de PHP. http://www.php.net/manual/es/#index