UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

INTEGRACIÓN DE SISTEMAS MAC OS X EN LA INFRAESTRUCTURA DE DIRECTORIO DEL INSTITUTO DE INGENIERÍA DE LA UNAM

I N F O R M E D E T R A B A J O

QUE PARA OBTENER EL TITULO DE
INGENIERO EN COMPUTACIÓN

MEDIANTE LA MODALIDAD DE
TRABAJO PROFESIONAL

PRESENTA
LUIS ALBERTO ARELLANO FIGUEROA

AVAL
DR. LUIS ÁLVAREZ-ICAZA LONGORIA

MÉXICO D.F. - 2014

Índice General

Índice de Figuras

CAPÍTULO 2

CAPÍTULO 3

CAPÍTULO 4

Índice de Tablas

CAPÍTULO 4

Estructura

El presente trabajo está dividido en varios capítulos que proporcionan un orden lógico a la información expuesta, esperando que mediante esta estructura el lector pueda acceder a la misma de una forma rápida, facilitando así su consulta bibliográfica.

Participación profesional

En esta sección se hace una presentación de mi participación profesional en este proyecto y el crecimiento profesional que he experimentado desde que ingresé a la Facultad de Ingeniería y durante los casi 20 años que he laborado en el Instituto de Ingeniería de la UNAM.

Objetivo

En este apartado se plantea el objetivo que me motivó para la realización de este trabajo

Introducción

Este punto presenta un panorama general de la evolución de las Tecnologías de la Información en el Instituto de Ingeniería de la UNAM y la forma en la que ha respondido a los nuevos cambios tecnológicos.

Capítulo 1 - Definición del problema

En este capítulo se trata la problemática observada con la incursión de equipos de cómputo con sistema operativo Mac OS X en el Instituto de Ingeniería, UNAM y se plantea una serie de elementos que deben ser resueltos por la implementación de la solución.

Capítulo 2 - Antecedentes

Este capítulo documenta la organización del Instituto de Ingeniería y de su Coordinación de Sistemas de Cómputo. De igual forma, se presenta una visión general de la organización del servicio de directorios ya implementado en el Instituto.

Capítulo 3 - Marco teórico

Durante este capítulo se hace un resumen de conceptos teóricos que son necesarios para comprender mejor el problema y que intervendrán durante el proceso de implantación de la solución.

Capítulo 4 - Análisis y metodología empleada

A lo largo de este capítulo se detalla el análisis realizado a las diferentes soluciones disponibles para la integración de Mac OS X con Active Directory, la selección de la mejor opción y el proceso de implementación.

Conclusiones

En este apartado se hace un resumen del trabajo realizado y de cómo el Instituto de Ingeniería utiliza el resultado de este proyecto en su beneficio.

Resultados y aportaciones

Esta sección presenta los resultados obtenidos después de la implantación de la solución, así como los beneficios obtenidos en el Instituto de Ingeniería, tanto para la Coordinación de Sistemas de Cómputo como para los usuarios.

Apéndice

El apéndice de este trabajo incluye el código fuente en Apple Script que se desarrolló durante la ejecución de este proyecto, y que sirve para automatizar el proceso de unión a dominio de los equipos cliente con sistema operativo Mac OS X a la infraestructura de Active Directory del Instituto de Ingeniería de la UNAM.

Participación profesional

En esta sección se hace una presentación de mi participación profesional en este proyecto y el crecimiento profesional que he experimentado desde que ingresé a la Facultad de Ingeniería y durante los casi 20 años que he laborado en el Instituto de Ingeniería de la UNAM.

Como Jefe del Área de Servidores Windows del Instituto de Ingeniería, desde el año 1999, me he especializado en tecnologías Microsoft y he trabajado en la implementación de soluciones empresariales de toda índole que involucran a la plataforma de Microsoft como el diseño de arquitecturas cliente y servidor con Windows, Active Directory, Exchange Server, SQL Server, SharePoint Server, entre otros.

Desde mi ingreso al Instituto en el año 1994 como estudiante sin estipendio, fui asignado al área de soporte técnico por la experiencia empírica que tenía de sistemas operativos DOS y fue en esta área en donde amplié y adquirí nuevos conocimientos, principalmente los relacionados con sistemas UNIX (Solaris) y redes de computadoras. Con el paso del tiempo mi interés se centró en el sistema operativo Windows, ya que era el sistema más utilizado y, día con día, se integraban más computadoras personales con este sistema a la red del Instituto, además de que a mi parecer Windows es un sistema operativo muy interesante con características avanzadas para proporcionar excelentes soluciones.

Al ser un estudiante de licenciatura de la Facultad de Ingeniería en la carrera de Ingeniería en Computación, que a la vez realizaba prácticas en el Instituto de Ingeniería, poco a poco tuve la oportunidad de ir aplicando los conocimientos adquiridos en la Facultad en el Instituto de Ingeniería, conocimientos que me permitieron cambiar la experiencia empírica por el análisis y metodologías de ingeniería que permiten la resolución de problemas bajo un enfoque más profesional.

El conocimiento adquirido a lo largo de mis estudios en la Facultad de Ingeniería con materias como “Computadoras y Programación” y “Programación Estructurada y Características de Lenguajes”, me proporcionaron las bases para la elaboración de programas para la automatización de algunas tareas repetitivas en el proceso de configuración de equipos; sin embargo fueron las materias de “Sistemas Operativos”, “Organización de Computadoras”, “Redes de Computadoras” “Organización y Administración de Centros de Cómputo” y “Temas Especiales de Computación (Seguridad Informática)” las que me marcaron e hicieron que mi interés se enfocara a buscar una especialización en la gestión e implementación de nuevas tecnologías, así como a las operaciones de TI.

Desde el año 1996 implementé el primer servicio de Directorio en el Instituto de Ingeniería al percatarme de la necesidad de reducir las llamadas de soporte que manejaba la CSC y desde ese entonces este servicio se transformó en la parte medular de la infraestructura de cómputo del Instituto. Esto me llevó a buscar especializarme en este tipo de arquitecturas logrando obtener varias certificaciones avaladas por Microsoft como son “Microsoft Certified Professional (MCP)”, “Microsoft Certified Systems Administrator (MCSA)” y “Microsoft Certified Systems Engineer (MCSE)”.

A partir del año 1999 el coordinador de Sistemas de Cómputo creó el Área de Servidores Windows (Página 26), para la cual fui designado como el jefe de esta y así poder

continuar mi trabajo con sistemas Microsoft, pero también para implementar e integrar nuevas tecnologías de forma agnóstica al fabricante, por lo que mis responsabilidades se ampliaron y estas abarcan desde la administración de servidores, hasta las tecnologías de audio y video, pasando por la seguridad informática y las bases de datos.

Actualmente tengo las siguientes responsabilidades a mi cargo en el Instituto de Ingeniería: administración del Directorio institucional, administración de servicios esenciales de red como DNS, DHCP y RADIUS, definición y aplicación de directivas de seguridad en equipos cliente, administración del servicio de correo electrónico, administración de los servidores de sitios Web y portales de colaboración, administración de servidores de impresión y NAS[1], administración de los sistemas de almacenamiento masivo SAN[2], administración del firewall perimetral, administración del sistema antimalware en clientes, administración del IPS [3] perimetral, administración de los servidores de Bases de Datos SQL, aprovisionamiento automatizado de sistemas operativos y aplicaciones en equipos cliente a través de la red, administración y operación de los sistemas de Videoconferencia, administración y operación del servicio de streaming, entre otros.

Por toda esta experiencia que he tenido la fortuna de ir adquiriendo en el Instituto de Ingeniería, a finales del año 2011 se me confió la tarea de trabajar en la integración de la plataforma Mac OS X a la infraestructura actual de Directorio que previamente había implementado y de cuya administración soy responsable hasta la fecha.

La implementación de la integración del sistema Mac OS X con Active Directory y la divulgación a los usuarios de las mejores prácticas para su uso, representó un nuevo reto para mi desarrollo profesional, pues se trata de un sistema operativo que a pesar de tener bastantes similitudes con Windows, también tiene diferencias muy marcadas al tratarse de un sistema UNIX.

Para este proyecto estuve dedicado al cien por ciento en un inicio al aprendizaje del funcionamiento del sistema operativo Mac OS X, sobre todo para familiarizarme con la interfaz gráfica, las herramientas de configuración gráficas y las herramientas de línea de comandos más utilizadas para automatizar y cubrir actividades que no se pueden hacer gráficamente.

Posteriormente trabajé en la integración con Active Directory, principalmente aplicando los conceptos de redes como DNS, LDAP y Kerberos, pero sin limitarme a ello exclusivamente, pues también realicé una serie de avances sobre la instalación remota de Mac OS X a través de la red utilizando el protocolo NetBoot/NetInstall, el anuncio y configuración de servicios automáticamente mediante el protocolo Bonjour, que está basado en la iniciativa Zeroconf de la IETF, y la implementación de Apple Remote

[1] Network Attached Storage – Almacenamiento Compartido en Red
[2] Storage Area Network – Red de Área de Almacenamiento
[3] Intrusion Prevention System – Sistema de Prevención de Intrusos

Desktop para la administración remota, recolección de inventarios y distribución de software de forma centralizada.

Finalmente, considero importante resaltar que el éxito de este proyecto lo atribuyo a la aplicación de los conocimientos que adquirí a lo largo de mi formación en la Facultad de Ingeniería de la UNAM, que incluyó la mezcla ideal de una preparación teórica y práctica, además de formación ética y de disciplina a la que todo ingeniero se debe ceñir.

Objetivo

El objetivo de este trabajo consistió en diseñar una infraestructura de cómputo que permitiera la integración de sistemas Mac OS X al servicio de Directorio de la red de datos del Instituto de Ingeniería de la UNAM para obtener el máximo aprovechamiento de los recursos de red disponibles proporcionando una integración robusta que brinde acceso transparente a los servicios y optimizando su utilización.

Para esto, se trabajó en implantar la tecnología adecuada que permitiera proporcionar el soporte técnico adecuado a la comunidad del Instituto de Ingeniería de la UNAM, con base en la aplicación de las mejores prácticas de administración de sistemas Apple y utilizando todos los recursos disponibles en el área de tecnologías de la información.

Introducción

Este punto presenta un panorama general de la evolución de las Tecnologías de la Información en el Instituto de Ingeniería de la UNAM y la forma en la que ha respondido a los nuevos cambios tecnológicos.

El Instituto de Ingeniería de la UNAM es uno de los centros de investigación con más prestigio en el país, que se dedica a la investigación aplicada en diversas áreas de la ingeniería.

Desde su fundación, el Instituto de Ingeniería se ha enfocado a la generación de nuevos conocimientos y técnicas que contribuyen al desarrollo, implementación y mantenimiento de sistemas físicos y teóricos, para resolver problemas que afectan a la sociedad mexicana.

La extensa comunidad de ingenieros que forman parte del Instituto utiliza la ciencia y herramientas tecnológicas para la resolución de problemas concretos mediante la elaboración de modelos matemáticos, diseños y tecnologías que se adaptan a las necesidades sociales, industriales e incluso económicas.

La complejidad de los retos modernos para encontrar soluciones de ingeniería, ha ocasionado que la comunidad del Instituto forme grupos interdisciplinarios que participan en distintos proyectos auspiciados por la industria privada, gobierno y la propia Universidad.

Estos retos y la integración de distintas áreas de conocimiento, apremiaron al Instituto a adoptar nuevas tecnologías como el cómputo, para acelerar el procesamiento de datos, hacer más eficiente el almacenamiento de información y agilizar la colaboración; por lo que creó la Coordinación de Sistemas de Cómputo y la designó como el ente encargado de diseñar, implementar y mantener la infraestructura de cómputo del Instituto.

La rápida adopción de computadoras personales entre la comunidad del Instituto, hizo que la Coordinación de Sistemas de Cómputo comenzara a trabajar desde sus inicios, en proveer una infraestructura de red robusta que interconectara estos equipos, pero a la vez, se hizo presente la necesidad de proporcionar servicios centralizados a través de servidores dedicados.

La evolución de los servicios de red, poco a poco llevó a la necesidad de optimizar los recursos disponibles, pero también a pensar en la implementación de sistemas que facilitaran el uso de estos servicios por parte de los usuarios y mejoraran las capacidades de administración de los mismos por parte de la Coordinación de Sistemas de Cómputo.

Uno de los principios básicos de una red distribuida moderna, implica el uso de un sistema de Directorio que permita la centralización de la autenticación de usuarios para reducir la carga de trabajo de los administradores y para hacer transparente el acceso a los usuarios.

El Instituto de Ingeniería cuenta con este sistema de Directorio desde 1996, el cual ha evolucionado a través de los años para convertirse en una parte esencial en las

actividades de su comunidad y para la implementación de nuevas tecnologías o sistemas.

El uso del Directorio facilita a los usuarios la localización de recursos de red, entre los que se encuentran otros usuarios, carpetas compartidas, servicios de impresión, etc.; mientras que a los administradores y desarrolladores los habilita con herramientas adecuadas para simplificar sus actividades de monitoreo, mantenimiento y control de acceso a recursos que deben tener ciertas restricciones.

Durante las últimas dos décadas el Instituto había homologado su infraestructura de cómputo a una plataforma de cómputo personal que esencialmente estaba orientada al sistema operativo Windows y esto funcionó correctamente por estar alineado a las tendencias mundiales para las áreas de tecnologías de la información.

Sin embargo, durante los últimos años, las tecnologías de la información han sufrido cambios enormes, sobre todo debido al aceleramiento del surgimiento de nuevas tecnologías como los dispositivos móviles, y esto ha colocado en posiciones de ventaja tecnológica a nuevos jugadores en la industria del cómputo, además de que los nuevos dispositivos han reducido los costos de la tecnología, haciéndola accesible a un número mayor de personas.

Esto ha obligado a la industria a adoptar nuevos paradigmas de trabajo como es el uso de equipos o dispositivos personales en el área de trabajo (BYOD[1]), la virtualización, el cómputo móvil y el uso de nubes públicas y privadas entre otros, y a partir de estas nuevas tecnologías se ha hecho imprescindible la instauración de ambientes heterogéneos.

Estos cambios no son excluyentes de la Universidad y mucho menos del Instituto de Ingeniería, que se ha caracterizado por mantenerse a la vanguardia tecnológica en todas sus áreas de investigación y que ahora se enfrenta a nuevos retos para mantener su infraestructura de cómputo congruente con las nuevas exigencias de sus usuarios.

Uno de los cambios importantes que se han presentado es el rompimiento del ambiente homogéneo que se tenía, para dar paso a nuevos sistemas operativos como Linux y Mac OS X, siendo el segundo el sistema operativo con mayor crecimiento en uso por parte de la comunidad del Instituto.

Dada esta situación, la Coordinación de Sistemas de Cómputo inició una serie de proyectos para la adecuación de la infraestructura de cómputo del Instituto a los nuevos modelos de TI[2] que involucran la adopción de nuevas tecnologías y su integración con la infraestructura existente para mantener la optimización, el monitoreo y la seguridad de los recursos y la información de la institución.

[1] Bring Your Own Device
[2] Tecnologías de la Información

Capítulo 1
Definición del Problema

En este capítulo se trata la problemática observada con la incursión de equipos de cómputo con sistema operativo Mac OS X en el Instituto de Ingeniería, UNAM y se plantea una serie de elementos que deben ser resueltos por la implementación de la solución.

Durante los últimos 18 años, el Instituto de Ingeniería ha basado su infraestructura de cómputo principalmente en la plataforma Microsoft, con una base instalada de equipos cliente con el sistema operativo Windows que alcanza el 85% y un porcentaje similar en servidores que se aproximan a la cantidad de 65.

Desde hace 3 años el Instituto ha visto crecer entre su comunidad la demanda de equipos con el sistema Mac OS X para su uso en actividades académicas, y la adquisición de este tipo de sistemas ha aumentado rápidamente, alcanzando un 10% de la base instalada de equipos cliente.

Esto ocasionó que el Instituto de Ingeniería a través del Área de Servidores Windows y Mac de la Coordinación de Sistemas de Cómputo, se planteara la necesidad de ampliar la infraestructura de cómputo actual con los elementos necesarios que permitieran integrar este tipo de equipos y así mantener el nivel de servicio a los usuarios en cuestión de soporte técnico, soporte de aplicaciones e integración con el esquema de autenticación del Instituto.

Para la integración de equipos Mac OS X a la infraestructura del Instituto, consideré como objetivo que se debería tomar en cuenta la facilidad de uso y operación de estos sistemas tanto por parte de los usuarios y el personal de soporte técnico, además de poder contar con los mecanismos necesarios para mantener el control de estos y así poder optimizar los recursos y mantener la seguridad de la red en niveles óptimos, por lo que se plantearon los siguientes puntos a cubrir.

1) Implementar un mecanismo sencillo para unir equipos Mac OS X a un Dominio de Active Directory.
2) Poder retirar los equipos Mac OS X de un Dominio de Active Directory cuando se requiera.
3) Sustituir el inicio de sesión local de los usuarios mediante la autenticación con Active Directory utilizando Kerberos.
4) Contar con la capacidad de migrar fácilmente las cuentas de usuario locales a cuentas de Dominio.
5) La solución debe permitir la distribución de configuraciones mediante grupos de Dominio y con la facilidad de los GPOs de Active Directory.
6) Ofrecer la capacidad de utilizar grupos de Active Directory para la asignación de permisos en el sistema de archivos de forma local (ACLs[1]) y para carpetas compartidas.
7) Los equipos cliente deberán tener la capacidad de usar credenciales en caché cuando los equipos Mac OS X estén desconectados.
8) Minimizar el impacto que pueda generar el software que se requiera instalar en clientes y servidores, y en general sobre la infraestructura actual del servicio de Directorio del Instituto.

[1] Access Control Lists – Listas de Control de Acceso

Capítulo 2
Antecedentes

Este capítulo documenta la organización del Instituto de Ingeniería y de su Coordinación de Sistemas de Cómputo. De igual forma, se presenta una visión general de la organización del servicio de directorios ya implementado en el Instituto.

2.1 Instituto de Ingeniería, UNAM

El Instituto de Ingeniería es uno de los centros de investigación en diversas áreas de la ingeniería que forma parte del Subsistema de la Investigación Científica de la Universidad Nacional Autónoma de México (UNAM).

Desde sus inicios, se ha dado a la tarea de realizar investigación orientada a problemas generales de la ingeniería, colaborando con entidades públicas y privadas, siempre buscando mejorar la práctica de la ingeniería en el ámbito nacional proporcionando servicios de ingeniería a los diversos sectores de la sociedad.

Además de las actividades de investigación, el Instituto de Ingeniería ha dedicado buena parte de sus esfuerzos a la formación de recursos humanos y a la difusión de los resultados de sus investigaciones, contribuyendo así al desarrollo del país.

El prestigio del Instituto de Ingeniería es ampliamente reconocido mediante la amplia variedad de convenios de investigación que tiene con empresas o corporaciones, y por la gran capacidad de los integrantes de su comunidad que está conformada por casi 100 investigadores, una cantidad similar de técnicos académicos, una población oscilante de más de 500 estudiantes que realizan trabajos de tesis de licenciatura, maestría y doctorado, y 140 personas del área administrativa.

En sus albores el Instituto se enfocó a resolver problemas que atañen a la ingeniería civil, pero en la actualidad cerca de la mitad de los miembros del Instituto provienen de disciplinas distintas de esta área e incluyen una mezcla de las distintas disciplinas de la ingeniería moderna.

Actualmente el Instituto de Ingeniería trabaja en tres grandes grupos de investigación que comprenden a la ingeniería estructural, desde la sismología, geotecnia y dinámica de las estructuras hasta la elaboración de normas constructivas urbanas; la ingeniería hidráulica y ambiental, que incluye la dinámica de fluidos, la biorremediación y los procesos biológicos del ambiente; y la ingeniería electromecánica, que abarca la automatización, los sistemas, la instrumentación y la ingeniería en computación (hardware y software), con grupos emergentes en manejo de bases de datos, seguridad informática, inteligencia artificial y las telecomunicaciones.

Esto ha hecho que el Instituto preserve su importante función de hacer ingeniería de calidad, original, útil y altamente competitiva, para resguardar su papel de árbitro nacional de la ingeniería y actor principal del desarrollo tecnológico, al mismo tiempo de que apoya a la docencia y la formación de expertos mediante la vinculación con la industria, el desarrollo de nuevas tecnologías y la colaboración con instituciones afines.

a. Organización

El Instituto de Ingeniería agrupa a sus diferentes áreas de investigación y operación de acuerdo con el siguiente organigrama funcional (Figura 2-1), en el que destacan sus tres Secretarías y tres Subdirecciones, por albergar al grueso de su población académica y estudiantil.

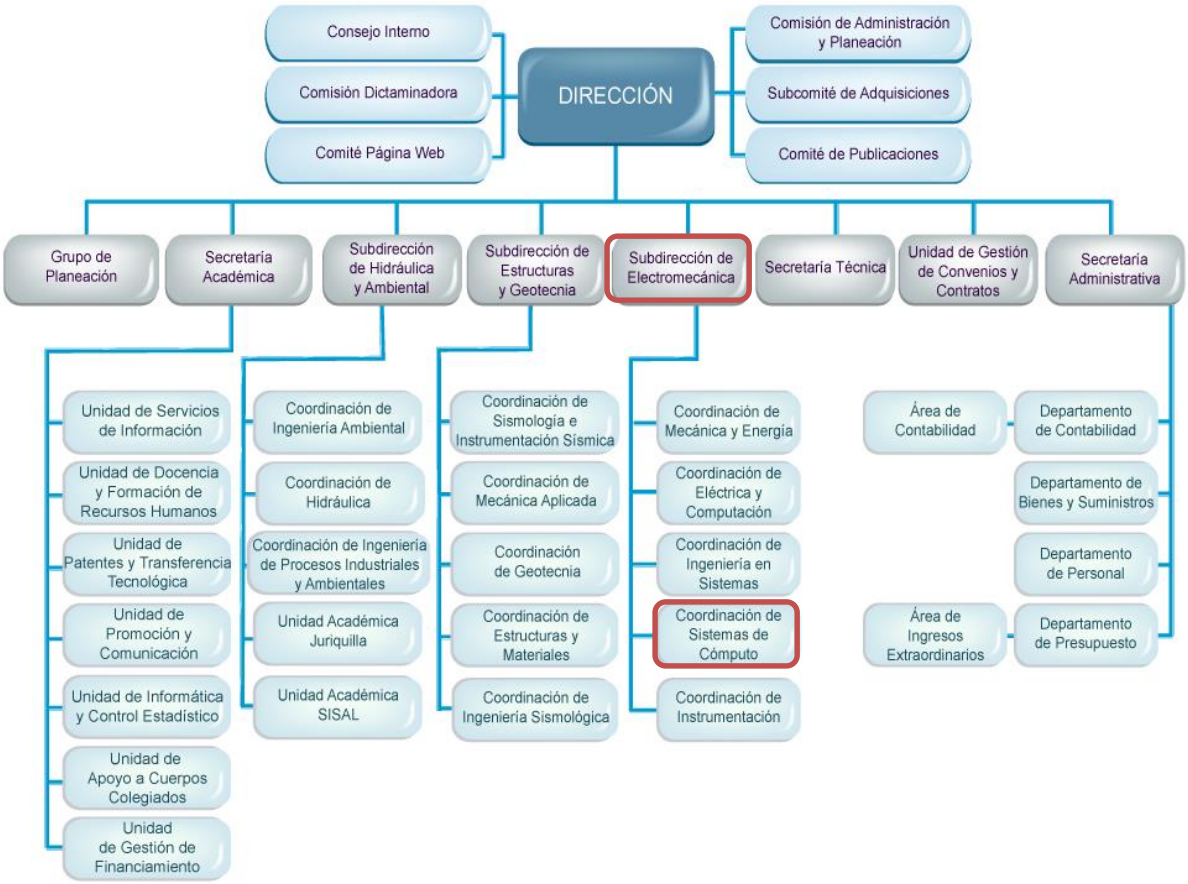

Figura 2-1 Organigrama del Instituto de Ingeniería, UNAM

b. Instalaciones

El Instituto de Ingeniería tiene instalaciones (Figura 2-2) que ocupan 15 edificios en la zona de Ciudad Universitaria, en la Ciudad de México, con una extensión de 26,020 metros cuadrados construidos entre laboratorios, cubículos, áreas comunes y un auditorio y además posee dos Unidades foráneas en Juriquilla, Querétaro y Sisal, Yucatán.

Edificio 1
"Fernando Hiriart Balderrama" •• Dirección • Secretaría Académica • Secretaría de Planeación y Desarrollo Académico • Secretaría Administrativa • Coordinación de Sismología e Instrumentación Sísmica Unidad de Promoción y Comunicación • Laboratorio de Instrumentación Sísmica • Unidad de Servicios de Información (USI). Biblioteca •

Edificio 2
Subdirección de Estructuras y Geotecnia • Coordinación de Estructuras y Materiales • Coordinación de Mecánica Aplicada •

Edificio 3
"Raúl Sandoval Landázuri" •• Laboratorio de Estructuras y Materiales • Laboratorio de Hidráulica •

Edificio 4
"Raúl Marsal Córdova" •• Coordinación de Geotecnia • Laboratorio de Mecánica de Suelos •

Edificio 5
Subdirección de Hidráulica y Ambiental • Coordinación de Hidráulica • Coordinación de Ingeniería Ambiental • Laboratorio de Ingeniería Ambiental •

Edificio 6
"Fernando Espinosa Gutiérrez" •• Coordinación y Laboratorio de Vías Terrestres •

Edificio 7
"Nabor Carrillo Flores" •• Laboratorio de Mecánica de Rocas • Laboratorio de Enrocamientos • Laboratorio de Microscopía Electrónica •

Edificio 8
Laboratorio de Hidromecánica • Laboratorio de Ingeniería Marítima • Laboratorio de Flujo Bifásico •

Edificio 9
Mesa Vibradora • Laboratorio de Geoteledetección •

Edificio 10
(Hangar) •• Laboratorio de Ingeniería Ambiental • Laboratorio de Gasificación •

Edificio 11
Modelos Hidráulicos •• Laboratorio de Modelos Fluviales •

Edificio 12
"Bernardo Quintana Arrioja" •• Subdirección de Electromecánica • Coordinación de Sistemas de Cómputo • Coordinación de Instrumentación • Coordinación de Ingeniería de Sistemas • Coordinación de Eléctrica y Computación• Coordinación de Mecánica y Energía • Taller Mecánico • Laboratorio de Doble Altura

Edificio 13
"Torre de Ingeniería" •• Laboratorio de Transporte y Sistemas Territoriales • Grupo de Sistemas Educativos • Coordinación de Mecánica y Energía • Grupo de Hidromecánica • Coordinación de Ingeniería Sismológica • Coordinación de Ingeniería de Procesos Industriales y Ambientales • Laboratorio de Geoinformática • Secretaría Técnica •

Basamento de la Torre de Ingeniería
Coordinación de Mecánica Aplicada • ala Norte Grupo Mecánica Numérica. Túnel de Viento • Ala Sur • Grupo de Ingeniería Lingüística • Grupo de Sismología • Grupo de Saneamiento de Suelos•

Edificio 18
Laboratorio de Control de Vibraciones en Edificios • Laboratorio de Electrónica de Potencia • Laboratorio de Pruebas no Destructivas • Laboratorio de Telecomunicaciones • Laboratorio de Energías Renovables y Diseño Bioclimático • Aulas de Uso Múltiples •

Unidad Académica Juriquilla
Unidad Académica Juriquilla • Laboratorio de Procesos Avanzados y Tratamiento de Aguas • Laboratorio de Análisis Físico-Químicos •

Unidad Académica SISAL
•Laboratorio de Ingeniería y Procesos Costeros•

Figura 2-2 Instalaciones del Instituto de Ingeniería, UNAM

2.2 Coordinación de Sistemas de Cómputo

La Coordinación de Sistemas de Cómputo (CSC) forma parte de la Subdirección de Electromecánica del Instituto de Ingeniería (Figura 2-1) y desde su formación en 1989 se ha dedicado a apoyar al personal académico en diversos proyectos de investigación, propiciando que la convergencia y el uso de las tecnologías de cómputo, informática, telecomunicaciones y microelectrónica, se asimilen y aprovechen como una herramienta de cambio.

La CSC trabaja en diversos temas de cómputo y telecomunicaciones, y se ha convertido en un agente importante dentro del Instituto para operar como una palanca de modernización e innovación que mejora la productividad de la comunidad en general.

Entre los temas tecnológicos en los que la CSC se ha involucrado, se encuentra el estudio de sistemas operativos, el supercómputo, las redes de telecomunicaciones convergentes, la ingeniería de software, el desarrollo Web, la telefonía IP, la educación a distancia, el diseño de bases de datos, el cómputo móvil y los sistemas de audio y video digitales.

Para cubrir de forma adecuada cada una de las áreas tecnológicas que abarca el cómputo, la CSC se ha organizado en varias áreas de trabajo, lo que le permite generar grupos de conocimiento especializado que respondan de forma ágil a las demandas actuales del Instituto y a su vez le facilita la formación de recursos humanos que se dediquen a la investigación y aplicación de nuevos conocimientos.

a. Organización

La Coordinación de Sistemas de Cómputo está organizada en 7 áreas, entre las cuales se encuentra el Área de Servidores Windows y Mac, que es el área en la que se desarrolló este proyecto (Figura 2-3).

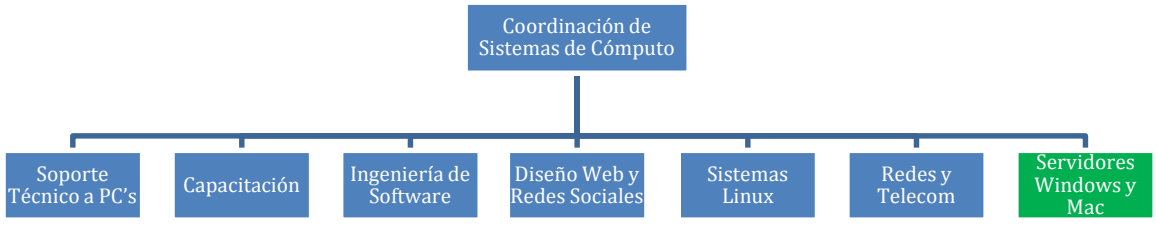

Figura 2-3 Organigrama de la Coordinación de Sistemas de Cómputo

1. Área de Soporte Técnico a PC's
   Esta área es la encargada de atender a los usuarios del Instituto en la resolución problemas cotidianos que involucran la instalación de software, configuración de sistema operativo, instalación de dispositivos como impresoras o tarjetas de expansión, y en general la resolución de problemas sobre la plataforma Windows.

2. Área de Capacitación
   Está dedicada a la elaboración de planes de capacitación interna e impartición de cursos de software de uso general a la comunidad del Instituto.

   De igual forma, esta área está incursionando en la elaboración de material educativo en video para ser publicado en redes sociales o transmitido por streaming.

3. Área de Ingeniería de Software
   Esta área se dedica al desarrollo de sistemas de escritorio y web, además de aplicaciones móviles que son de uso interno o como apoyo en la realización de proyectos a cargo de otras áreas de investigación del Instituto.

   El trabajo del área de Ingeniería de Software implica el desarrollo y mantenimiento de aplicaciones administrativas internas que requieren un conocimiento profundo de los procesos de operación del Instituto, hasta el desarrollo de aplicaciones que recolectan, difunden y generan información de carácter científico que son utilizadas por otras coordinaciones del Instituto y otras dependencias universitarias y sus patrocinadores.

4. Área de Diseño Web y Redes Sociales
   Esta área se encarga de la creación y mantenimiento de los diferentes sitios web públicos y privados que tiene el Instituto, que incluyen el portal Web público, el sitio de la Intranet, sitios Web de los distintos proyectos de investigación, páginas de congresos y sitios de colaboración interna o interinstitucionales. Todo esto considerando la parte creativa, mediante el desarrollo de la imagen gráfica de los sitios Web y el tratamiento de video que se difunde por streaming bajo demanda.

   Además, en esta área de lleva a cabo la administración y publicación de la información que se difunde en las distintas redes sociales públicas en las que tiene presencia el Instituto.

5. Área de Sistemas Linux
   Esta área se encarga de mantener la infraestructura de servidores Linux del Instituto y de proporcionar el soporte técnico necesario a los usuarios de este sistema operativo.

Trabaja en áreas del cómputo como la virtualización, la implementación de herramientas de uso científico y el desarrollo de portales Web, además de administrar uno de los dos servicios de correo electrónico del Instituto.

De igual forma, se encarga de administrar y optimizar el uso de un cluster de supercómputo que corre sobre la plataforma Linux y que sirve como apoyo a distintos grupos de investigación del Instituto de Ingeniería para la ejecución de aplicaciones de propósito científico y que les permite acelerar la obtención de resultados necesarios para sus estudios.

6. Área de Redes y Telecomunicaciones
   En esta área se mantiene y administra la infraestructura física de la red del Instituto de Ingeniería, al igual que el sistema de telefonía que utiliza VoIP.

   Los integrantes de esta área están a cargo del diseño, planeación y administración del cableado estructurado en las instalaciones del Instituto y de los equipos de red involucrados en la comunicación como son switches Ethernet de capa 2 y 3, puntos de acceso y switches inalámbricos, transceivers, etc.

   También se encargan de la implementación de la segmentación de redes mediante VLANs, el ruteo interno de VLANs y la asignación del direccionamiento IP interno y externo.

7. Área de Servidores Windows y Mac
   Esta es el área que dirijo desde el año 1999 y es la responsable de llevar a cabo la implementación de los servicios de red esenciales para la administración y operación de la red del Instituto, como son los servicios de resolución de nombres DNS y WINS, el servicio DHCP para asignación de direcciones IP y el realm Kerberos, así como el Directorio institucional basado en Active Directory.

   Además está encargada de la administración de los recursos de archivos e impresión que se comparten en red, mediante la implementación de servidores dedicados utilizando las plataformas Windows y Mac OS X.

   Esto hace que opere como un pilar de apoyo para las otras áreas de la CSC, al proporcionar los servicios necesarios para el alojamiento de sitios y portales web, la implementación y puesta en producción de aplicaciones desarrolladas internamente, la implementación de tecnologías para la transmisión por secuencias de audio y video (streaming), el diseño de estrategias de distribución de sistemas operativos y aplicaciones de forma automatizada a través de la red, la instauración de ambientes de prueba para desarrollo y en general el control de las operaciones de TI.

   Esta área se especializa en la investigación de nuevas tecnologías y en diseñar los esquemas necesarios que permitan que sean adoptadas por la comunidad del

Instituto. Entre los temas que desarrolla actualmente, están la virtualización de escritorios, la consolidación de servidores mediante virtualización, el diseño de centros de datos, el supercómputo, el manejo de grandes volúmenes de datos y la implementación de redes sociales corporativas.

El área también se dedica a mantener y operar la seguridad informática interna y perimetral del Instituto mediante la ejecución de análisis seguridad en equipos cliente, y la implementación y administración del firewall e IPS perimetrales, así como de la red de videoconferencia del Instituto mediante la administración de 6 salas dedicadas a este propósito.

Todas estas áreas están regidas por un Coordinador de Sistemas de Cómputo, quien es el responsable de coordinación de estas áreas de trabajo, la asignación de recursos y la asignación de proyectos, además de reportar directamente al Subdirector de Electromecánica.

2.3 Infraestructura de Directorio del Instituto de Ingeniería, UNAM

El Instituto de Ingeniería ha confiado la planeación, diseño, implementación y operación de su infraestructura de red, a la Coordinación de Sistemas de Cómputo desde el año 1989, por lo que se ha beneficiado con la integración de sus servicios y operaciones a través de una sola instancia que provee soluciones integrales y con una visión y planeación unificada.

El Área de Servidores Windows y Mac de la CSC ha puesto en operación una infraestructura integral que desde hace años ha permitido que la comunidad académica del Instituto aumente su productividad al abstraerles la carga de la operación de una red de datos compleja y en constante cambio, y siempre ha procurado proporcionar tecnología de punta que mantenga a la vanguardia los procesos de investigación que el Instituto desarrolla.

Unos de los puntos esenciales para las operaciones de red del Instituto fue la implementación de un Directorio institucional que desde el año 2000 puse en operación utilizando la plataforma de Active Directory.

La cantidad de equipos que asciende a casi 1,000 y el creciente número de usuarios de aproximadamente 1,500, hace prácticamente imposible pensar en mantener un esquema de trabajo monolítico, y es por esto que se decidí implementar un Directorio que permitiera la autenticación centralizada y el control distribuido de configuraciones en los equipos de cómputo cliente y servidores.

Actualmente se tiene una infraestructura de Active Directory formada por un Dominio maestro y diecisiete Dominios de recursos, mediante los cuales se realiza la autenticación de usuarios y equipos, e igualmente se distribuyen directivas de uso de los recursos de red para usuarios y directivas de configuración para los equipos de cómputo.

Esta estructura de Dominios (

Figura 2-4) está definida por el organigrama funcional del Instituto para que corresponda con sus distintas áreas de trabajo, en especial las Coordinaciones; por lo que el Dominio maestro representa a la institución y los Dominios "hijo" o de recursos, representan a la Dirección, las Secretarías y cada una de las Coordinaciones.

Los Dominios de recursos son utilizados para alojar las cuentas de los equipos de cómputo de cada área de trabajo del Instituto, que se integran mediante una unión autenticada al Dominio correspondiente, pero no contienen cuentas de usuario.

Cada Dominio de recursos distribuye mediante Group Policy una serie de directivas de configuración a los equipos que se le han unido; una directivas han sido planeadas para responder a las necesidades globales de seguridad y homogeneidad del Instituto, y otras directivas se aplican de forma local de acuerdo con las necesidades y lineamientos de cada una de las áreas de trabajo.

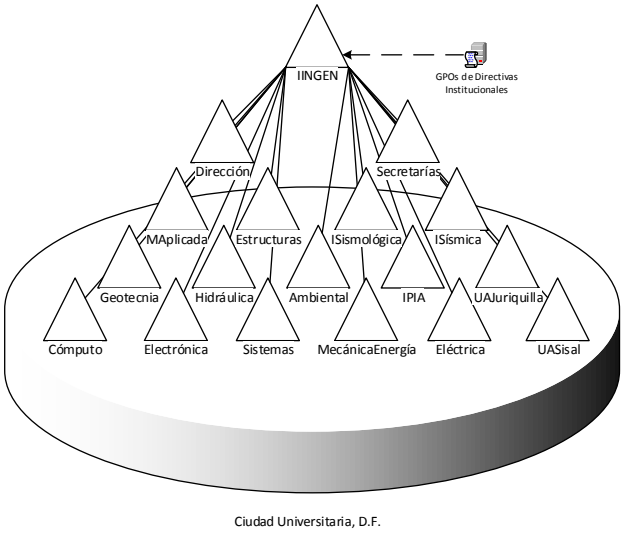

Figura 2-4 Estructura de Dominios del Instituto de Ingeniería para la Ciudad de México

El Dominio maestro se encarga de concentrar la totalidad de las cuentas de usuario de la comunidad del Instituto, por lo que es el Dominio que se encarga de realizar la autenticación y de validar el acceso a los recursos de red al formar el origen del Realm de Kerberos. En este Dominio las cuentas de usuario también son organizadas de acuerdo con el organigrama funcional del Instituto mediante Unidades Organizativas para la asignación de directivas de Group Policy que permiten aplicar configuraciones de usuario de una forma más granular.

El nombre que se asignó al Dominio maestro corresponde con el dominio DNS que tiene asignado el Instituto, para simplificar la administración de los recursos y facilitar a los

usuarios la identificación de los mismos. Para lograr esta coexistencia de dominios, se tiene implementado un servicio interno de DNS que sigue los principios de un "Split DNS" al complementarse con el servicio de DNS de la UNAM provisto por la DGTIC.

El servicio interno de DNS tiene la autoridad de las zonas iingen.unam.mx e ii.unam.mx, y de los subdominios que se originan a partir del Dominio IINGEN; en estas zonas se almacenan los registros de todos los servidores y todas las computadoras cliente del Instituto, mediante la actualización dinámica para sistemas Windows y Mac OS X y mediante registros estáticos para sistemas Linux.

Los equipos del Instituto localizan algunos de los recursos de red a través del servicio de DNS interno mediante solicitudes de resolución de nombres para ubicar la dirección IP de un servidor en particular, pero también para identificar mediante registros SRV, las direcciones IP de los servidores de autenticación LDAP, los servidores KDC de Kerberos, los servidores con el rol de Catálogo Global y los recursos compartidos mediante el protocolo Bonjour de servidores Apple.

Para sistemas y usuarios ubicados en Internet, es el servicio de DNS administrado por la DGTIC el que les responde y resuelve los nombres de los servidores del Instituto, y este solamente contiene un subconjunto de los registros que se tienen en el servicio de DNS interno, ya que solamente se registran los servidores que ofrecen servicios externos.

Otro mecanismo implementado en el Instituto y mediante el cual se resuelven los nombres de los equipos para obtener su dirección IP, es el servicio WINS, el cual mantiene limpios de broadcasts los segmentos de red y permite que se tenga comunicación entre equipos en distintos segmentos de red mediante el protocolo NetBIOS, que por diseño no puede ser ruteado.

La infraestructura de Directorio del Instituto de Ingeniería, está implementada de forma tal que ofrece una alta disponibilidad mediante mecanismos de cómputo distribuido y redundancia a fallos; por lo que se cuenta con suficiente hardware especializado distribuido a través de las distintas ubicaciones geográficas en donde el Instituto tiene presencia.

En las instalaciones de Ciudad Universitaria se tienen implementados tres servidores Windows Server 2012 R2 que ejecutan el rol de AD DS para formar el Dominio maestro IINGEN, y al mismo tiempo operan como servidores de DNS para resolución interna y como servidores WINS para resolución NetBIOS. Estos servidores mantienen una base de datos de Active Directory independiente, pero que es replicada de manera permanente y constante entre sí, por lo que si uno de los servidores llegase a fallar, las operaciones de autenticación no se verían afectadas. Para el servicio de WINS se mantiene un diseño similar con bases de datos independientes que se replican cada 10 cambios o cada 15 minutos.

El servicio de DNS es un caso especial, ya que este también se mantiene actualizado mediante la replicación de la información que almacena, pero no utiliza los mecanismos tradicionales de transferencia de zonas que define el RFC, sino que la replicación está supeditada a los mecanismos de replicación de Active Directory al almacenar sus zonas en una partición de este servicio de Directorio, por cuestiones de rendimiento, compatibilidad y seguridad.

Adicionalmente, se tienen dos servidores Windows Server 2008 R2 que mediante virtualización con Hyper-V ejecutan instancias de 34 servidores que actúan como Controladores de Dominio para la Dirección, Secretarías y las Coordinaciones del Instituto; diecisiete de estos servidores se ejecutan en un servidor de virtualización para formar los dominio y los otros diecisiete se ejecutan en el segundo servidor para proporcionar controladores de dominio redundantes, que mantienen una réplica entre ellos y brindan la redundancia suficiente para que las actividades del Instituto no se afecten.

En las instalaciones de las sedes foráneas del Instituto, se tienen implementados dos centros de datos que alojan servidores que proporcionan los servicios básicos de red para que la comunidad que ahí labora pueda desempeñar correctamente sus actividades, y entre los servicios críticos e indispensables están los servicios de Directorios, DNS y WINS.

En la Unidad Académica Juriquilla se tienen dos servidores Windows Server 2012 R2 que actúan como Controladores de Dominio del Dominio IINGEN y por lo tanto replican sus bases de datos con los servidores centrales de Ciudad Universitaria. Además se tienen dos servidores de virtualización con Hyper-V que alojan servidores de infraestructura como un servidor de impresión, DHCP y al Dominio UAJuriquilla, que opera con dos Controladores de Dominio adicionales a los implementados en el sitio central (

Figura 2-5).

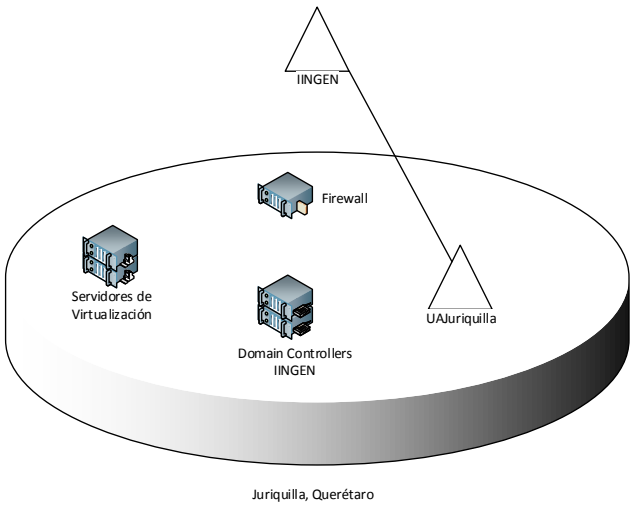

Figura 2-5 Estructura de Dominios del Instituto de Ingeniería para la Unidad Académica Juriquilla

En la Unidad Académica Sisal se implementaron dos servidores con Hyper-V para virtualización en los que se ejecuta la totalidad de la infraestructura que da servicio a esta sede foránea del Instituto, y en estos se tienen de igual forma dos servidores virtuales que fungen como Controladores de Dominio para el Dominio IINGEN y dos servidores Controladores de Dominio para el Dominio UASisal (

Figura 2-6), todos ellos manteniendo un calendario de replicación de una hora con el sitio central ubicado en CU.

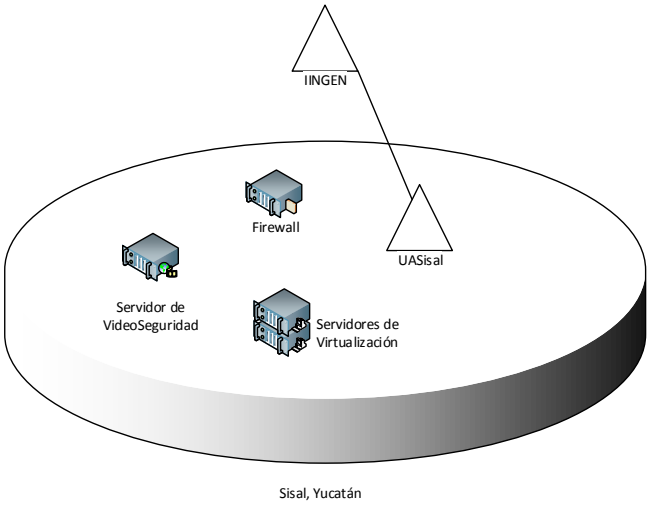

Figura 2-6 Estructura de Dominios del Instituto de Ingeniería para la Unidad Académica Sisal

El hardware utilizado en los servidores de Ciudad Universitaria, Juriquilla y Sisal, tiene los elementos indispensables de redundancia para prevenir la interrupción en sus operaciones en caso de una falla de hardware, como son fuentes de energía redundantes, discos duros configurados en RAID1 para los volúmenes del sistema operativo y RAID5 para los volúmenes de datos, esto aplica especialmente para el almacenamiento de máquinas virtuales en el caso de los servidores con Hyper-V. Además, estos servidores cuentan con tecnología “hotplug”, que permite el cambio de discos duros, fuentes de energía y ventiladores sin necesidad de apagarse.

Capítulo 3
Marco Teórico

Aquí se hace un resumen de conceptos teóricos que son necesarios para comprender mejor el problema y que intervendrán durante el proceso de implantación de la solución.

3.1 Servicios de directorio

En la actualidad prácticamente todo el mundo que hace uso de computadoras depende de que sus equipos estén conectados a través de una red de datos para poder compartir y tener acceso a información a través de aplicaciones distribuidas. Esta información debe estar organizada de forma clara y consistente para mejorar su facilidad de uso, funcionalidad y reducir costos de administración.

La información que describe a usuarios, aplicaciones, servicios, archivos, impresoras y otros recursos accesibles a través de una red de datos, a menudo es almacenada en una base de datos especial llamada Directorio y es posible consumirla por medio de un modelo cliente-servidor en el que un cliente de directorio solicita la búsqueda de información a un servidor de directorio y este último es el responsable de hacer la búsqueda en todo el Directorio para entregarla al solicitante.

a. Directorio

Un Directorio es un conjunto de información de objetos almacenada con un orden determinado para proporcionar detalles de cada objeto.

Un ejemplo clásico de un Directorio es el directorio telefónico que acostumbran distribuir en la ciudades las compañías telefónicas; en este directorio telefónico se almacena el nombre de las personas en forma alfabética (objetos) y se les asocia su número telefónico y su dirección (características), de igual forma este directorio suele contener una sección en la que se listan negocios o profesiones en la llamada sección amarilla. Cuando se desea consultar la información de este directorio solo basta con buscar el nombre de la persona o el nombre del negocio o profesión para obtener toda la información necesaria para contactarlos.

Este comportamiento de un Directorio se puede plasmar perfectamente en sistemas de cómputo para poder almacenar objetos que representen usuarios, computadoras u otros dispositivos como impresoras y para poder utilizarlos en un ambiente de red.

Un Directorio permite a usuarios o aplicaciones encontrar recursos con características particulares para la realización de alguna tarea. Por ejemplo, un usuario puede buscar impresoras que estén ubicadas en el mismo piso en el que trabaja, que tenga papel tamaño oficio y que cuente con la capacidad de imprimir a doble cara.
Un términos generales, un Directorio es una base de datos especializada y es muy diferente a las bases de datos relacionales de propósito general, pues esta base de datos está optimizada para la lectura y búsqueda de información y relega la escritura de nueva información ya que se considera una operación limitada para uso de los administradores del directorio.

Debido a que un Directorio está diseñado para almacenar información relativamente estática y está optimizado para este propósito, un Directorio no es la herramienta adecuada para almacenar información que cambia constantemente y de forma muy rápida. Para este propósito se sigue haciendo necesario el uso de bases de datos relacionales.

Además de las diferencias en optimización de lectura y escritura que tiene un Directorio con respecto a las bases de datos relacionales, existen otras diferencias que vale la pena mencionar.

1) Los Directorios comúnmente no soportan transacciones y si las soportan, son transacciones de todo a nada.
2) Los Directorios suelen estar limitados en el tipo de datos que almacenan y no suelen almacenar colecciones arbitrarias de datos.
3) Otra diferencia es la forma de obtener la información, pues comúnmente las bases de datos relacionales utilizan lenguajes muy poderosos como SQL [1], mientras que los Directorios utilizan protocolos simplificados y optimizados para la velocidad como LDAP[2].

b. Directorios Distribuidos

Dependiendo de su implementación, los Directorios puede ser centralizados o distribuidos.

Si solamente se tiene un servidor de directorio que aloja la información, se dice que el Directorio es centralizado, y cuando se tiene más de un servidor de directorio para tener acceso a la información, se habla de que el Directorio es distribuido.

Cuando un Directorio es distribuido, la información que almacena puede ser particionada o replicada. Si la información se particiona, cada servidor de directorio almacena un subconjunto de la información que no se repite entre sí; y cuando la información se replica, la misma información del Directorio se almacena en cada servidor de directorio.

c. Beneficios de los Servicios de Directorio

La implementación de Servicios de Directorio en una red de cómputo, indudablemente proporciona beneficios importantes a cualquier organización, ya que simplifican la administración de la red y de los equipos, además de que simplifican la experiencia de los usuarios.

Con los Servicios de Directorio, pueden mantener centralizada la información de todos los usuarios, contraseñas, ubicación de archivos en red, impresoras, computadoras e incluso otras redes de datos.

Al almacenar este tipo de información de forma centralizada se obtienen los siguientes beneficios:

1) Se reduce la complejidad en la captura de información.

[1] Structured Query Language – Leguaje de Consultas Estructurado
[2] Lightweight Directory Access Protocol – Protocolo Ligero de Acceso a Directorios

2) Se tiene la certeza de que la información sobre usuarios y recursos en consistente.
3) Se simplifica la administración de usuarios y recursos de red.
4) Se puede contar con la capacidad de dotar de servicios de identificación, autenticación y autorización a diferentes servicios de red.

3.2 Estándares para el Acceso a Directorios

En la década de los años setenta comenzó el apogeo de nuevas tecnologías de comunicación que se basaban en sistemas de cómputo, pero en aquella época los diferentes fabricantes de tecnología construían sistemas propietarios que eran incompatibles con otros sistemas, por lo que se hizo evidente que era necesario generar estándares que permitieran la interacción e integración de estos sistemas, y esto dio origen a dos grupos que emitieron estándares para intentar cubrir esta necesidad.

Uno de estos grupos fue dirigido por la CCITT[1] (ahora ITU-T[2]) y la ISO[3], las cuales trabajaron para dar origen al Modelo de Referencia OSI[4], el cual definió un modelo de siete capas para la comunicación de datos.

El otro grupo fue encabezado por la DARPA y a través del Grupo de Trabajo de Ingeniería de Internet (IETF[5]) generó una serie de estándares para Internet mediante la publicación de documentos llamados Petición de Comentarios (RFC - Request for Comments)

a. X.500

En 1988 la CCITT creó el estándar X.500 para cubrir los Servicios de Directorios mediante el modelo OSI.

X.500 define la organización de elementos en un Directorio, las capacidades de búsqueda para facilitar la extracción de información del Directorio y la comunicación entre los clientes y el Servicio de Directorio.

El principio básico de operación de X.500 consiste en la generación de una organización jerárquica de objetos llamada Árbol de Información del Directorio (DIT – Directory Information Tree) que es almacenada de forma distribuida en uno o más servidores llamados Agentes del Sistema del Directorio (DSA – Directory System Agents) y que son consultados por aplicaciones llamadas Agentes de Usuario del Directorio (DUA – Directory User Agents).

[1] Comité Consultatif International Téléphonique et Télégraphique
[2] International Telegraph Union – Telecommunication Standardization Sector
[3] International Standards Organization
[4] Open Systems Interconnect
[5] Internet Engineering Task Force

Cada objeto contiene un conjunto de atributos que a su vez pueden tener uno o más valores. A estos objetos se les asigna un único Nombre Distintivo (DN - Distinguished Name) formado por la combinación de su Nombre Distintivo Relativo (RDN - Relative Distinguished Name) más uno o varios atributos del objeto y el RDN de cada objeto superior hasta alcanzar la raíz del DIT.

De igual forma, X.500 definió una serie de protocolos que utilizaban las capas del modelo OSI, entre los cuales se incluyen los siguientes:

1) DAP - Protocolo de Acceso al Directorio (Directory Access Protocol)
2) DSP - Protocolo de Servicios del Directorio (Directory Service Protocol)
3) DISP - Protocolo de Replicación de Información del Directorio (Directory Information Shadowing Protocol)
4) DOP - Protocolo de Operaciones de Directorio (Directory Operations Protocol)

Un problema con la adopción del estándar X.500 fue su complejidad y la gran cantidad de recursos necesarios para su implementación en la época de su publicación.

b. LDAP

El Protocolo Ligero de Acceso a Directorios (LDAP) fue diseñado por la Universidad de Michigan y originalmente fue pensado como una alternativa al protocolo DAP de los clientes por la necesidad de contar con una alternativa menos compleja y que redujera la carga de los clientes con respecto al protocolo DAP que permite el acceso a Directorios X.500.

LDAP utiliza una arquitectura cliente-servidor que transporta sus mensajes a través de TCP/IP en lugar del modelo OSI, y fue diseñado para simplificar algunas de las operaciones de X.500, incluso mediante la omisión de varias funciones complejas de este protocolo, y con el tiempo evolucionó para también sustituir al protocolo DSP que es la parte servidor de X.500.

El modelo de nombres de LDAP define la forma en la que los objetos son organizados e identificados, ya que utiliza la misma estructura de árbol DIT de X.500. Esto quiere decir que en LDAP cada objeto tiene un nombre llamado Nombre Distintivo (DN) que está formado por una secuencia de Nombres Distintivos Relativos (RDN) que siguen la jerarquía del DIT.

La simplicidad de LDAP ha ocasionado que sea aceptado ampliamente como el método de acceso a directorios en Internet y por lo tanto se ha convertido en un elemento indispensable en las Intranets de muchas organizaciones, siendo LDAPv3 la versión más reciente y utilizada.

La arquitectura de LDAP está definida en los RFC 2251, 2252, 2253, 2254, 2255 y 2256 en los que se crearon una serie de modelos básicos que permiten su implementación y que se resumen a continuación.

i. Modelo de Información

Este modelo define la creación de elementos en el Directorio y las características que los harán únicos.

La unidad básica de información que se almacena en el Directorio es llamada Objeto y su función es representar objetos de la vida real como personas, servidores, computadoras, impresoras, organizaciones, etc.

Los Objetos están formados por un conjunto de Atributos que contienen información sobre él y cada Atributo puede tener uno o más Valores pero un solo Tipo de información (Figura 3-1).

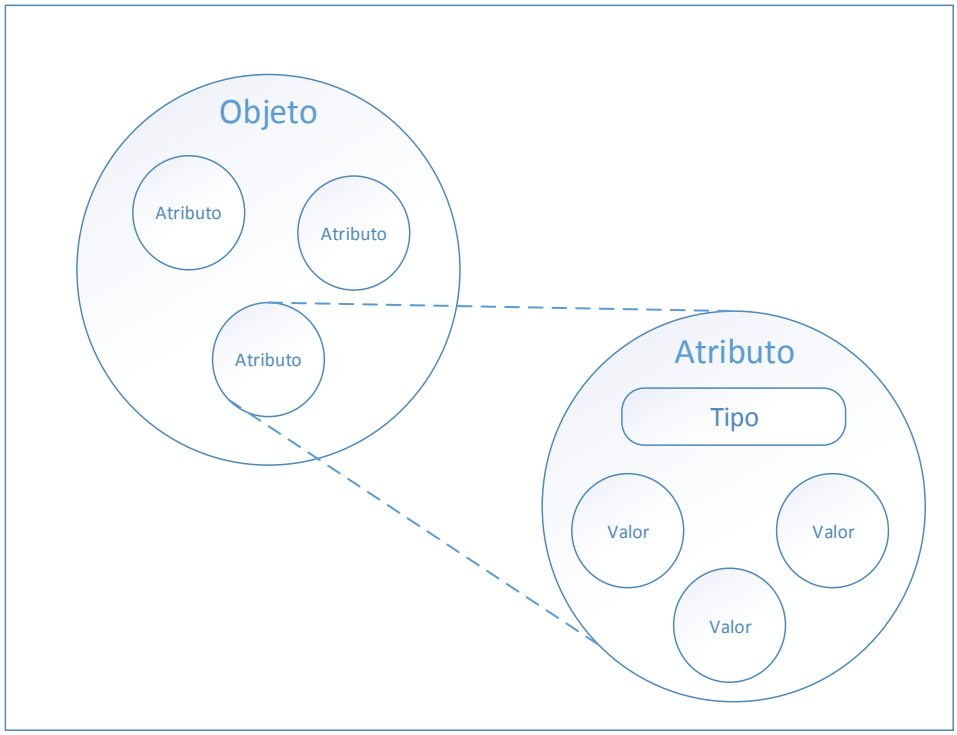

Figura 3-1 Elementos de un Objeto

El Tipo de un Atributo está asociado a una Sintaxis que define el patrón de información que puede ser almacenada en sus Valores y también determina el comportamiento de los Valores durante las búsquedas u otras operaciones de directorio.

Para determinar y acotar los tipos de Objetos que se pueden almacenar en el Directorio se definió el Esquema, que además mantiene una lista de los Atributos de cada Objeto e indica cuándo un Atributo es opcional u obligatorio.

El Esquema certifica la consistencia de datos en el Directorio al asegurarse que ningún Objeto será almacenado si no cuenta con los Atributos elementales o que no se almacenarán Atributos de Objeto que no estén definidos por él. Además, el Esquema

define la jerarquía o estructura del DIT en la que se almacenan los Objetos, así como la herencia y las subclases de los Objetos mismos.

Una Subclase es el resultado de formar Objetos a partir de otros Objetos y consiste en crear un Objeto que integre los mismos Atributos de una Clase de Objeto pero agregando un número pequeño de Atributos que lo hagan exclusivo, por lo que este nuevo Objeto heredará la mayoría de los Atributos de un Objeto superior. Existe una clase de objeto especial llamada Top que no tiene superiores.

Todos y cada uno de los Objetos del Directorio incluyen un Atributo especial llamado objectClass cuyo Valor será uno o más nombres de Esquema que representan el Tipo de Objeto que representan. Entre los valores que puede tener objectClass están Top o Alias, se utiliza Alias para definir que el Objeto es un seudónimo de otro Objeto o Top para definir que el Objeto está en la cima de la jerarquía y tiene Objetos subordinados.

Al igual que objectClass, existe otra clase de objeto llamada extensibleObject que hace a un Objeto capaz de almacenar cualquier atributo y se utiliza para agregar Atributos especiales a pocos Objetos sin la necesidad de generar una nueva clase de objeto. Esta capacidad debe tratarse con mucho cuidado ya que un Objeto podría incluir cualquier tipo de información y generaría conflictos o desorden en un sistema estructurado como es el Directorio.

Una Clase de Objeto define los tipos de Objetos en un Directorio como pueden ser una persona, organización, unidad organizacional y un componente de dominio, de igual forma una Clase de Objeto puede definir la relación de un Objeto con otros Objetos, un ejemplo sería la clase Top que indica la relación del Objeto con sus subordinados en forma de una estructura de árbol jerárquica.

Una Clase de Objeto define también los Atributos obligatorios y los Atributos opcionales de los Objetos, estos Atributos pueden ser coincidentes o redundantes con los de otras Clases de Objeto, por lo que en LDAP es común que un Objeto esté definido por varias Clases de Objeto.

Las Clases de Objeto pueden ser definidas de tres formas:

1) Abstractas
   Usada como plantilla para crear otras Clases de Objeto.

2) Estructurales
   Se utilizan para instanciar Objetos de Directorio

3) Auxiliares
   Pueden adjuntarse a Objetos instanciados por Clases de Objeto estructurales y sirven para extender una Clase de Objeto estructural sin modificar su definición en el Esquema.

La estructura del registro de una Clase de Objeto comienza con un número llamado Identificador de Objeto (OID – Object Identifier) seguida del Nombre (NAME) y Descripción (DESC) de la Clase de Objeto, a continuación se agrega la Clase de Objeto superior (SUP) en caso de ser subordinada de otra Clase de Objeto, y finalmente se agregan los Atributos obligatorios (MUST) y opcionales (MAY).

Por ejemplo, la clase de objeto "top" está en la cima de la jerarquía y todas las Clases de Objeto que no estén planeadas para ser subordinadas de otra Clase, deberán tener a la Clase "top" como su superior.

objectclass: top
objectclasses=(2.5.6.0 NAME 'top' DESC 'Standard ObjectClass' ABSTRACT MUST (objectClass))

La Clase "person" se define como subordinada de la Clase "top" y requiere que los atributos cn (common name) y sn (surname) tengan definido un valor de forma obligatoria, mientras que de forma opcional, debe contener valores en los atributos userPassword, telephoneNumber, seeAlso y description.

objectclass: person
objectclasses=(2.5.6.6 NAME 'person' DESC 'Defines entries that generically represent people.' SUP 'top' STRUCTURAL MUST (cn $ sn) MAY (userPassword $ telephoneNumber $ seeAlso $ description))

Un Identificador de Objeto (OID) es una cadena numérica que sirve para identificar Objetos o Atributos de Objeto de forma única a nivel internacional y está formado por una serie de números separados por puntos. Cada uno de estos números forman parte de una jerarquía que es administrada por la ISO y la ITU, estas organizaciones delegan la administración de los OID a otras organizaciones al asignarles números OID y estas organizaciones pueden asignar OIDs a Objetos propios e incluso delegar nuevamente la administración a otras organizaciones asignándoles otro grupo de OIDs.

Los OIDs se forman por una cadena numérica inicial llamada raíz o vértice, y a la cual se le van agregando números de forma única para formar ramas o arcos, por ejemplo 1.5.2.3.9.15 es el vórtice y 1.5.2.3.9.15.1, 1.5.2.3.9.15.2, 1.5.2.3.9.15.3, 1.5.2.3.9.15.4, etc., son los arcos que pueden ser usados para asignarse a Objetos o para delegarlos a otras organizaciones que a su vez pueden generar nuevos arcos o ramas para su uso como 1.5.2.3.9.15.1.1, 1.5.2.3.9.15.1.2, 1.5.2.3.9.15.1.3, 1.5.2.3.9.15.1.4, etc.

El arco o rama inicial de una organización refleja la estructura jerárquica del OID a nivel global, por ejemplo 1.2.840.113612.5.4.2.5 es el OID asignado al proyecto UNAM Grid de la DGTIC (antes DGSCA) y se separa de la siguiente forma:

1 (OID asignado a ISO)
1.2 (Entidades miembro de ISO)
1.2.840 (Estados Unidos de América)
1.2.840.113612 (Energy Sciences Network – ESnet)
1.2.840.113612.5 (International Grid Trust Federation – IGTF)

1.2.840.113612.5.4 (Member Policy Management Authorities (PMA))
1.2.840.113612.5.4.2 (IGTF Member Issuing Authorities)
1.2.840.113612.5.4.2.5 (UNAM DSC, Grid Certification Authority)

Si una organización requiere agregar Clases de Objeto o Atributos propios a su Directorio, es recomendable que se obtenga un arco o rama de alguna organización autorizada como ISO, ITU o IANA para garantizar la interoperabilidad del Directorio

ii. Modelo de Nombres

Este modelo define cómo los Objetos son identificados y organizados en el Directorio.

LDAP organiza los Objetos en una estructura de árbol jerárquica llamada Árbol de Información del Directorio o DIT[1] (

Figura 3-2) y estos Objetos son organizados en el DIT de acuerdo con su Nombre Distintivo (DN).

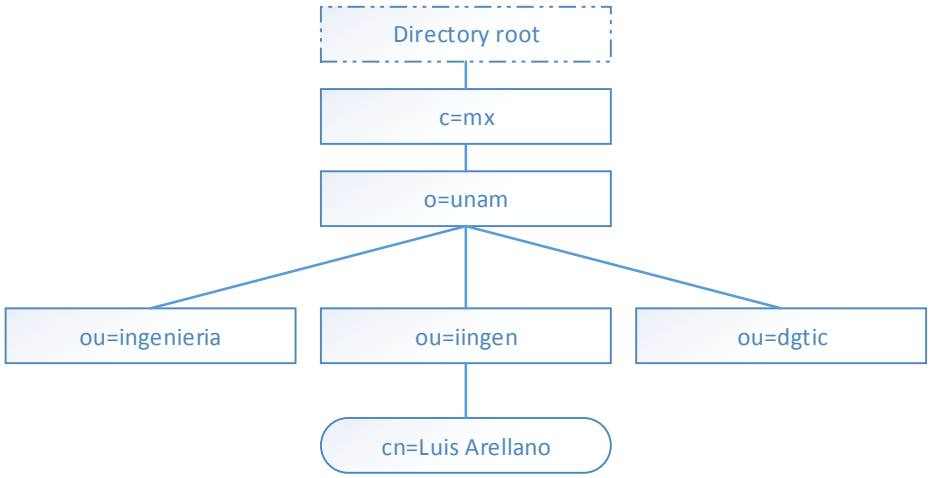

Figura 3-2 Árbol de Información del Directorio

Un DN es un nombre único que identifica a un Objeto de forma indudable y está formado por una secuencia de Nombres Distintivos Relativos (RDN) separados por comas.

Cada RDN es obtenido de un Atributo de un Objeto o una rama del DIT y está definido por <nombre del atributo> = <valor> y representa un punto dentro de la jerarquía de espacio de nombres del Directorio.

El DN de un Objeto se forma de izquierda a derecha correspondiendo a los RDN de la parte más profunda del árbol hasta llegar a la raíz.

[1] Directory Information Tree

iii. Modelo Funcional

Este modelo incluye tres categorías de operaciones que pueden ser llevadas a cabo en el Servicio de Directorio.

1) Autorización
   Incluye las operaciones de Vincular (Bind), Desvincular (Unbind) y Abandonar (Abandon) que sirven para realizar conexiones y desconexiones a servidores LDAP, establecer privilegios de acceso y proteger la información.

2) Consulta
   Incluye las operaciones Buscar (Search) y Comparar (Compare) para Objetos que cumplan con un criterio establecido por los usuarios.

3) Actualización
   Incluye las operaciones Agregar (Add) para crear Objetos, Borrar (Delete) para eliminar Objetos, Modificar (Modify) para cambiar Atributos en los Objetos y Modificar RDN (ModifyRDN) para cambiar el Nombre Distintivo Relativo de los Objetos.

iv. Modelo de Seguridad

Este modelo está ligado a la operación Vincular del modelo funcional de LDAP y define los mecanismos de seguridad para proteger la información sensible del Directorio que es transportada o actualizada a través de la red.

El paradigma de seguridad en sistemas informáticos comprende cuatro aspectos que se deben cubrir para poder mantener un sistema libre de inconvenientes y accesos no deseados.

1) Autenticación
   Asegura que el usuario es quién realmente dice ser.

2) Integridad
   Asegura que la información transmitida no es modificada en el transcurso de la transmisión.

3) Confidencialidad
   Previene la divulgación de información a usuarios que no deberían tener acceso a ella.

4) Autorización
   Asegura que el usuario tenga permitido llevar a cabo la acción que esté intentando hacer.

Hasta el momento el estándar LDAPv3 solamente cubre los aspectos de autenticación, integridad y confidencialidad, siendo necesario cubrir el aspecto de autorización con otros medios.

Las operaciones de Vinculación pueden utilizar diferentes mecanismos de seguridad para acceder a información del Directorio y los más relevantes son los siguientes:

1) Autenticación Anónima
   Es el método de autenticación más simple y se utiliza cuando se dejan vacíos los campos del DN y la contraseña durante una operación de Vinculación a LDAP.

2) Autenticación Básica
   Este método de autenticación es utilizado cuando se envía un DN y una contraseña en texto plano y estos coinciden con los que están almacenados en el Directorio. Obviamente no se recomienda el uso de este método de autenticación, ya que se corre el riesgo de que se vulnere la confidencialidad de la información transmitida.

3) Capa de Seguridad y Autenticación Simple (SASL[1])
   SASL es un marco de trabajo general en el que se dispone de diferentes métodos de autenticación para protocolos orientados a conexión, por lo que se puede definir a SASL como un sistema general que sirve para mediar entre protocolos y sistemas de autenticación, por ejemplo LDAP y Kerberos.

   Adicionalmente, SASL puede negociar la seguridad necesaria para cifrar los datos que se transmitan después de la autenticación, con lo que se asegura la confidencialidad de la información.

Además de estos mecanismos de seguridad, LDAPv3 define una extensión de protocolo llamada extensión de Seguridad de la Capa de Transporte (TLS – Transport Layer Security), que permite que las operaciones de Directorio sean cifradas para proteger la integridad y confidencialidad de las sesiones.

3.3 Kerberos

Kerberos es un protocolo de autenticación cuyo desarrollo inició en el año 1983 como parte del Proyecto Athena del Instituto de Tecnología de Massachusetts (MIT).

Las primeras tres versiones del protocolo solamente fueron usadas de forma interna en el MIT con fines de prueba y fue hasta la versión 4, que se distribuyó al público general en 1989, sin embargo su distribución y uso se limitó a los Estados Unidos de América debido a que el protocolo define el uso del algoritmo de cifrado DES y en esa época el gobierno estadounidense restringía la exportación de software de cifrado complejo.

La versión actual de Kerberos es la versión 5 que se definió en el RFC 1510 y a pesar de es una evolución de la versión 4 y que cubre la misma funcionalidad, Kerberos 5 fue rediseñado completamente y se puede decir que es una implementación nueva con

[1] Simple Authentication and Security Layer

código que no se parece en nada a la versión 4, lo cual permitió corregir deficiencias e incluir nuevas características.

El protocolo Kerberos se diseñó desde un inicio para ser una solución de red basada en un modelo cliente-servidor, que permitiera tener un inicio de sesión único en la red (SSO[1]) y cubrir los principios básicos de seguridad de sistemas como la autenticación, la integridad, la confidencialidad y el no repudio.

La principal característica de Kerberos es la autenticación a través de Boletos o Tickets de autenticación, que son asignados a los clientes para acceder a recursos de red como carpetas compartidas, correo electrónico, sitios Web y mensajería instantánea entre otros.

La implementación de Kerberos como sistema de autenticación permite eliminar el riesgo ancestral de los sistemas cliente-servidor como es la intercepción de contraseñas, la suplantación de clientes y servidores con ataques del tipo Man-in-the-Middle, ya que nunca envía información de autenticación en Texto Plano y siempre lleva a cabo una autenticación mutua.

La meta del protocolo Kerberos consiste en mejorar la seguridad y la facilidad para el usuario y se puede definir con los siguientes conceptos:

1) Seguridad
   Kerberos ofrece seguridad ya que nunca transmite contraseñas en texto plano y nunca envía contraseñas a través de la red para probar la identidad de un usuario ante algún servidor y en su lugar envía Tickets que utilizan mensajes criptográficos limitados por tiempo.

2) Inicio de Sesión Único
   Esta característica permite que los usuarios solamente inicien sesión para poder tener acceso a recursos de red, una vez que el usuario ha sido autenticado al iniciar sesión, este es autenticado de forma transparente mediante Tickets ante los servicios de red que soporten Kerberos.

3) Confianza de un Tercero
   En una infraestructura de red con Kerberos, todas las peticiones de autenticación son orquestadas por un servidor Kerberos centralizado en el cual todos los equipos de la red confían.

4) Autenticación Mutua
   La autenticación mutua no solo permite identificar al usuario que intenta acceder a un recurso de red, sino que también provee la certeza de que el servidor al que se hace la conexión es el correcto.

[1] Single Sign-On

Para cumplir con los conceptos anteriores, Kerberos debe mantener segura la comunicación entre los equipos de la red y para ello hace uso de dos elementos:

1) Cifrado
   El Cifrado de información permite transformar un mensaje de forma tal que solamente las partes involucradas que tengan la llave de Descifrado puedan leer el contenido original, lo cual mantiene la confidencialidad de la información en ambientes cliente-servidor y redes distribuidas en las que cualquiera puede escuchar el tráfico transmitido (Sniff).

   Kerberos soporta varios algoritmos de Cifrado para lograr la confidencialidad de sus comunicaciones, entre los que se encuentran DES, 3DES, AES y RC4, siendo DES el algoritmo más ampliamente soportado, pero que rápidamente está siendo remplazado por AES o RC4 que es el algoritmo que Microsoft está utilizando en sus más recientes implementaciones de Kerberos.

2) Integridad
   La Integridad de Mensajes permite asegurar que un mensaje transmitido a través de la red no sea modificado durante el tránsito a su destino, normalmente se busca que esta verificación sea confiable y fácil de decodificar, por lo que desde hace tiempo se han diseñado diversos algoritmos de Integridad de Mensajes.

   Los algoritmos de Integridad de Mensajes son llamados a menudo Hashes y son funciones matemáticas de un solo camino en las que se introduce un mensaje de entrada con longitud variable y se obtiene un mensaje de tamaño fijo que representa de forma única al mensaje de entrada, siendo muy fácil de calcular la salida a partir de la entrada pero matemáticamente difícil de calcular el mensaje de entrada a partir del mensaje de salida.

   Kerberos soporta varios algoritmos de Hash que van desde los más simples y débiles hasta los más fuertes con evasión de colisiones, como son los algoritmos CRC-32, MD5 y SHA.

a. Protocolo Needham-Schroeder

El protocolo Kerberos fue diseñado con los principios del protocolo Needham-Schroeder que fue publicado en 1978 por Roger Needham y Michael Schroeder de Xerox PARC[1], en el que se detalla la implementación de un servicio seguro de autenticación distribuida a través de criptografía de llave secreta.

El protocolo Needham-Schroeder define tres participantes en el intercambio de información durante la autenticación:

[1] Xerox Palo Alto Research Center

1) Cliente
   Es cualquier computadora que solicita la autenticación, usualmente es el equipo del usuario final.

2) Servidor de Aplicación
   Es cualquier servidor de aplicaciones o servicios al que el cliente desee conectarse.

3) Servidor de Autenticación
   Es un servidor dedicado que almacena las llaves de cifrado de todos los usuarios y servidores de la red, y es un servidor en el que todos confían.

El principio básico del protocolo Needham-Schroeder consiste en proveer un mecanismo para distribuir de forma segura una llave de cifrado de vigencia corta entre dos entidades para que estas puedan comunicarse mediante una transmisión de datos cifrados con dicha llave. Este mecanismo es esencial para evitar la transmisión de Contraseñas o Hashes en texto plano directamente al Servidor de Autenticación.

El proceso de autenticación definido por el protocolo Needham-Schroeder se lleva a cabo de la siguiente forma:

1) El Cliente contacta al Servidor de Autenticación enviándole un mensaje que contiene la identidad del Cliente, la identidad del Servidor de Aplicación al que desea acceder y un valor aleatorio llamado Nonce.

2) El Servidor de Autenticación recibe el mensaje inicial del Cliente y obtiene de su almacén de información las llaves de cifrado del Cliente y del Servidor de Aplicación; además genera una Llave de Sesión que será usada para establecer una comunicación segura entre el Cliente y el Servidor de Aplicación.

3) El Servidor de Autenticación envía un mensaje de respuesta al Cliente, formado por dos capas.

   En primer lugar, se crea un mensaje cifrado con la llave del Servidor de Aplicación que incluye la Llave de Sesión y el nombre del Cliente.

   Posteriormente este mensaje es empaquetado dentro de otro mensaje cifrado con la llave del Cliente y que incluye el nombre del Servidor de Aplicación, la Llave de Sesión y el Nonce originalmente enviado por el Cliente.

4) El Cliente recibe el mensaje de respuesta del Servidor de Autenticación y descifra la primera capa utilizando su llave de seguridad.

5) El Cliente envía al Servidor de Aplicación el mensaje que estaba envuelto en la primera capa de la respuesta del Servidor de Autenticación.

6) El Servidor de Aplicación recibe el mensaje enviado por el Cliente y lo descifra con su llave de seguridad, aceptándolo como válido y considera la conexión como autenticada correctamente.

7) El Servidor de Aplicación hace una verificación del Cliente mediante el envío de un método de desafío-respuesta (challenge-response) al enviarle un Nonce cifrado con la Llave de Sesión.

8) El Cliente recibe el mensaje del desafío, lo descifra y aplica una operación al Nonce.

9) El Cliente cifra el nuevo Nonce, lo cifra con la Llave de Sesión y lo envía de regreso al Servidor de Aplicación.

10) El Servidor de Aplicación recibe el mensaje del Cliente, lo descifra y verifica la operación sobre el Nonce, con lo que comprueba la identidad del cliente.

Una vez que se completa el proceso de autenticación, toda la comunicación que se lleva a cabo entre el Cliente y el Servidor de Aplicación se cifra con la Llave de Sesión, con lo que se previene cualquier tipo de ataque por manipulación, violación a la confidencialidad y suplantación.

b. Operación de Kerberos

El protocolo Kerberos está formado por varios elementos que están definidos por cierta terminología que es importante conocer para comprender a fondo su proceso de operación (Figura 3-3).

i. Realm

Un Realm o Reino es una frontera administrativa de control definida por uno o más servidores KDC[1] y por computadoras cliente.

Aunque no es obligatorio, por convención se suele utilizar como nombre del Realm el nombre del dominio DNS en mayúsculas, por ejemplo el dominio DNS iingen.unam.mx da lugar al Realm IINGEN.UNAM.MX

ii. Principal

Un Principal es un término que está asociado con un objeto de un Realm de Kerberos almacenado en el KDC y que representa a un usuario, un servicio o un equipo.

[1] Key Distribution Center – Centro de Distribución de Llaves

Un Principal está definido por tres partes, el nombre del usuario, servicio o equipo, el nombre de la instancia precedido por el símbolo "/" [opcional] y el nombre del Realm precedido por el símbolo "@", por ejemplo, LArellanoF[/admin]@IINGEN.UNAM.MX

iii. Llave

Cada Principal de Kerberos tiene asignada una Llave privada que solamente conocen él y el KDC, esta Llave es generada mediante una función de un solo sentido que se aplica a la contraseña del usuario para convertirla en una Llave de Cifrado binaria que será usada para cifrar y descifrar mensajes.

Durante el proceso de transformación de la contraseña a una Llave de Cifrado, entra en juego un elemento llamado "Salt", que es una secuencia de caracteres que se agrega a la contraseña antes de obtener el hash y tiene como objetivo el hacer única la Llave.

Para la versión 5 de Kerberos, el Salt que se emplea es el nombre del Realm, por lo que si un usuario utiliza la misma contraseña en dos Realms distintos y su Llave es comprometida en uno de los Realms, no se compromete la Llave del otro Realm.

iv. Ticket

Un Ticket es una estructura de datos cifrada que ha sido emitida por un KDC y que incluye una Llave de Cifrado única para cada sesión y varios campos que indican el alcance de uso del Ticket, la validez del Ticket y las capacidades e información del Principal.

Los Tickets sirven para confirmar la identidad de los participantes en una comunicación y para establecer una Llave de Cifrado de corta duración que ambas partes pueden compartir para asegurar la comunicación, llamada Llave de Sesión.

Los principales campos que se incluyen en un Ticket son:

- El nombre del Principal que lo solicita
- El nombre de servicio del Principal
- La expiración del Ticket
- Una lista de direcciones IP desde donde se puede usar el Ticket
- La Llave de Sesión (Llave de Cifrado de secreto compartido (shared secret)
- El tiempo de vida del Ticket

Los Tickets tiene un periodo de vida relativamente corto para minimizar el daño que se pudiese ocasionar en caso de que un atacante llegue a robar uno y normalmente duran entre 10 y 24 horas.

v. KDC

El Centro de Distribución de Llaves (Key Distribution Center) o KDC, es la parte esencial de cualquier Realm de Kerberos y su función es proveer los servicios de autenticación de Kerberos mediante a emisión de Tickets cifrados que requieren una Llave secreta para ser descifrados.

El KDC está formado por tres elementos lógicos que son una base de datos que almacena todos los Principals y sus Llaves de cifrado asociadas, un Servidor de Autenticación (AS) y un Servidor de Otorgamiento de Tickets (TGS), y aunque estos tres elementos están separados lógicamente, normalmente son implementados en un solo programa que los ejecuta en un único proceso.

Cada Realm de Kerberos puede tener varios KDC y debido a que cada uno de ellos tiene su propia base de datos, todos los KDC deben estar sincronizados para asegurar la consistencia de la autenticación, y al menos uno de ellos deberá siempre estar en operación para mantener su disponibilidad.

Los KDC deben estar altamente resguardados y deben mantener una configuración de seguridad lo más alta posible, ya que contienen las Llaves Secretas de cada Principal del Realm que son información sensible y crucial.

vi. Servidor de Autenticación (AS)

Este servidor emite un Ticket Granting Ticket o TGT a los clientes que desean iniciar sesión al Realm de Kerberos.

Durante el proceso de inicio de sesión al Realm el cliente nunca envía su contraseña al KDC y en lugar de ello solamente solicita un TGT. Este TGT es cifrado con la contraseña del cliente y debido a que solamente el cliente y el KDC conocen la contraseña, este podrá ser descifrado únicamente por la contraseña correcta del cliente.

El TGT es el responsable de brindar la capacidad de SSO[1] en Kerberos ya que una vez que el TGT es descifrado por el cliente, este puede ser utilizado para solicitar Tickets individuales de servicio, eliminando la necesidad al usuario de escribir su contraseña para cada servicio que contacte.

En Kerberos v5 se introduce un proceso adicional previo a que el AS emita un TGT que es llamado Autenticación Previa (Pre-Authentication), este proceso hace más difícil los ataques por fuerza bruta o por diccionario fuera de línea, y a los que eran susceptibles las versiones anteriores. Esta vulnerabilidad consiste en el hecho de que el KDC de las versiones anteriores de Kerberos emite un TGT para cualquier Principal a cualquier cliente que lo solicite, y como este TGT está cifrado con la Llave secreta del Principal se puede montar un ataque para determinarla, sobre todo cuando los usuarios utilizan contraseñas débiles.

La Autenticación Previa requiere que los solicitantes de TGTs prueben su identidad antes de que el KDC emita un Ticket para un Principal en particular. Cuando un cliente intenta adquirir un TGT, el KDC le envía un mensaje KRB_ERROR en lugar de un AS_REP como respuesta a la petición, esto le indica al cliente que debe autenticarse previamente por lo que el cliente genera los datos necesarios y vuelve a enviar la petición AS_REQ

[1] Single Sign-On – Inicio de Sesión Único

con los datos de autenticación adjuntados. Si la autenticación es aceptada por el KDC, este responde con el TGT, si la autenticación falla, el KDC vuelve a regresar un mensaje KRB_ERROR y no se emite el TGT.

vii. Servidor de Otorgamiento de Tickets (TGS)

Este servidor emite Tickets individuales de servicio a los clientes que los soliciten.

El TGS solicita al cliente dos datos: la solicitud de Ticket con el nombre de Principal que representa al servicio que se quiere contactar, y el TGT emitido por el AS. Una vez que el TGS verifica que el TGT es válido, emite el Ticket de servicio solicitado al usuario.

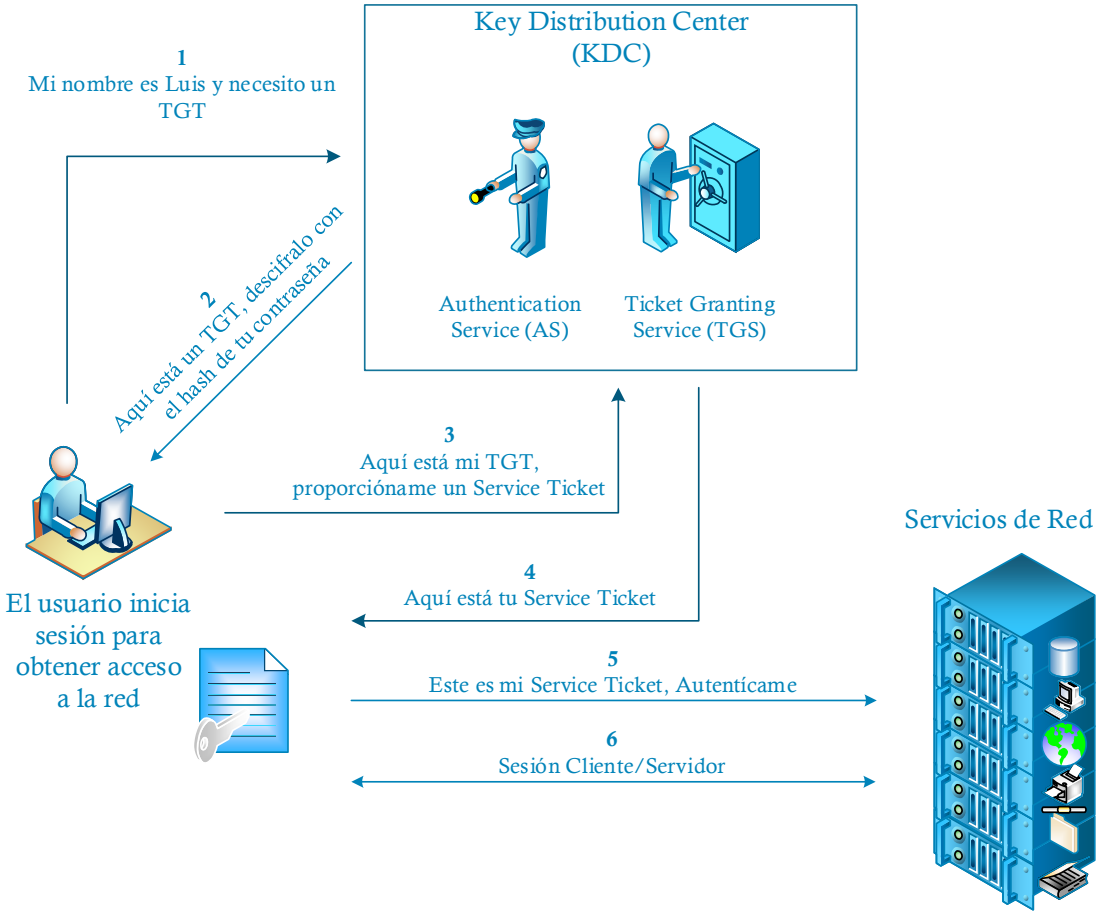

Figura 3-3 Intercambio de Tickets en Kerberos

3.4 Active Directory

Active Directory o Directorio Activo, es un servicio de directorio desarrollado por Microsoft que es utilizado comúnmente para la plataforma de clientes Windows y su estructura está basada en estándares abiertos como el protocolo Kerberos v5 definido en el RFC 1510[1] y el protocolo LDAP definido en el RFC 2307[2].

Este servicio de directorio provee la funcionalidad de una solución de identidad y acceso a redes, lo que lo hace un elemento esencial para proteger recursos como archivos, correo electrónico, bases de datos y aplicaciones.

Las funciones básicas de Active Directory son las siguientes:

1) Almacenar información de usuarios, computadoras y cualquier otra identidad.
   Active Directory provee un almacén de identidades, también conocido como Directorio, en el cual almacena objetos que interactúan con recursos de red.
   Estos objetos pueden ser usuarios, computadoras, grupos y servicios, los cuales tendrán propiedades asociadas a ellos como puede ser su nombre y su identificador de seguridad.
   El almacén de identidades es suministrado por un servidor que aloja y ejecuta el rol de Servicios de Directorio de Active Directory (AD DS) llamado Domain Controller y desde este mismo se administra.

2) Autenticar identidades.
   Active Directory lleva a cabo el proceso de autenticación que consiste en verificar peticiones de acceso solicitadas por una identidad.
   Para verificar una identidad, esta debe proporcionar un elemento secreto que solo es conocido por la propia identidad y la infraestructura de identidad y acceso mediante el almacén de identidades.

3) Controlar el acceso.
   El control de acceso a recursos se realiza mediante la infraestructura de identidad y acceso para proteger información confidencial de acuerdo a las directivas de cada organización.
   Para controlar el acceso a recursos se asignan permisos mediante listas de control de acceso (ACL) que especifican el nivel de acceso para cada identidad.

4) Proveer rastros para auditoría.
   Active Directory provee los mecanismos de auditoría necesarios para monitorear cambios o accesos a recursos por parte de una identidad y los almacena en registros que pueden ser consultados en cualquier momento.

[1] "The Kerberos Network Authentication Service (V5)"
[2] "An Approach for Using LDAP as a Network Information Service"

Además de los elementos básicos antes mencionados, Microsoft ha integrado una serie de componentes adicionales que consolidan su plataforma de identidad y acceso, proveyendo una infraestructura integral de seguridad que proporciona no solamente el manejo de identidades y control de acceso, sino también integridad y confianza en datos y entre organizaciones mediante servicios de certificados y administración de privilegios.

Adicionalmente, Active Directory ofrece mecanismos para administrar y configurar recursos en ambientes de red distribuidos mediante la asignación centralizada de directivas de administración, lo cual hace de este servicio una poderosa herramienta de administración de redes de cómputo.

a. Componentes de una Infraestructura de Active Directory

Una infraestructura de Active Directory está constituida por varios componentes que se definen por su función lógica o física.

1) Controlador de Dominio
   Es un servidor que aloja el servicio de directorio y ejecuta los servicios de administración de identidad y acceso dentro de una organización.
   Debido a que un Controlador de Dominio (DC) provee funcionalidad crítica para el control de acceso, la falla de este tipo de servidores puede ocasionar la pérdida de continuidad de las operaciones en una organización y por lo tanto se deberá considerar implantar al menos dos servidores que alojen el servicio de AD DS[1].

2) Sitios
   Un sitio es una ubicación física dentro de la infraestructura de red de una organización, como puede ser una oficina o una ciudad.
   Una organización puede tener uno o varios sitios, dentro de los cuales comúnmente implementa equipos de red que proveen una conectividad de buena calidad.
   En el caso de contar con varios sitios, es común que las organizaciones utilicen enlaces de red que los unan para integrar el acceso a recursos de red. Estos enlaces pueden variar en calidad y costo, y pueden ser tan básicos como un enlace dial-up o tan sofisticados con un enlace de fibra óptica.
   Active Directory proporciona una clase de objeto llamada "Site" mediante la cual se pueden generar objetos de Sitio que representan las redes de una organización con conectividad rápida y confiable.

   La segmentación de Active Directory en Sitios permite crear fronteras de replicación y facilita la localización de servicios de red, por ejemplo, los Controladores de Dominio replican la información de su almacén de datos en segundos cuando están en el mismo Sitio y en periodos controlados cuando están en diferentes Sitios con conexión poco fiable; de igual forma, cuando un

[1] Active Directory Directory Services

usuario inicia sesión, este es autenticado por un Controlador de Dominio ubicado en el mismo Sitio que su equipo de cómputo.

3) Almacén de Datos
   Es una base de datos que almacena las identidades de Active Directory y básicamente es un archivo llamado Ntds.dit que se aloja en el directorio %SystemRoot%\Ntds de los Controladores de Dominio.

   Esta base de datos está dividida en "particiones" que comprenden el esquema, configuración, catálogo global y el contexto de nombres del dominio; además de proveer "particiones de aplicación" para que aplicaciones o servicios almacenen datos que requieran ser replicados y que no estén relacionados directamente con los servicios de directorio.

4) Dominio
   Un Dominio es la unidad lógica básica de una infraestructura de Active Directory dentro de la cual se comparten características y capacidades entre los objetos pertenecientes al mismo y es necesario un Controlador de Dominio para poder crearlo.

   Entre otras cosas, un Dominio contiene datos de identidad de los usuarios, grupos y computadoras dentro de la partición de dominio del almacén de datos.

   Adicionalmente, un Dominio define un ámbito para la aplicación de directivas de administración de seguridad o configuración, por lo que al crear varios dominios en una organización es posible asignar diferentes directivas a los equipos de cómputo de acuerdo a lineamientos o necesidades específicas.

   Otra característica de los Dominios es la capacidad de segmentar el espacio de nombres de las identidades para adecuarlo a la estructura organizacional, facilitando su identificación.

5) Bosque
   Un Bosque es una colección de uno o más Dominios que contiene una única definición de la configuración de la red y una única instancia del esquema del directorio.

   En Active Directory el Bosque define la frontera de seguridad del directorio, ya que nunca se replicará información del mismo fuera de este límite.

   Cuando se crea el primer Dominio en una organización, se crea de forma implícita el Bosque y este Dominio es definido como el Dominio Raíz del Bosque.

6) Árbol
   Desde el momento en que se crea el primer Dominio de una organización se puede hablar de la existencia inherente de un Árbol y este Árbol puede crecer a través de la generación de Subdominios o se pueden generar Árboles nuevos con sus propios Subdominios.

   Los Árboles se definen por el espacio de nombres de DNS[1] de los Dominios y estos pueden ser contiguos o no contiguos.

   Cuando se tiene un Dominio raíz cuyo espacio de nombres es *unam.mx* y se genera un Subdominio *iingen.unam.mx*, estamos hablando de que estos dos Dominios forman parte del mismo Árbol ya que su espacio de nombres de DNS es contiguo.

   Por el contrario, si se tiene un Dominio raíz llamado *iingen.unam.mx* y se crea otro Dominio con el nombre *ingenieria.unam.mx*, estos se considerarán dos Árboles pues su espacio de nombres es no contiguo.

7) Unidad Organizacional
   Active Directory es una base de datos jerárquica que almacena Objetos, estos Objetos pueden ser agrupados en contenedores, que básicamente son una Clase.

   Una Unidad Organizacional (OU) es un tipo especial de contenedor que no solamente sirve para agrupar Objetos sino que además sirve como un ámbito de administración de los mismos mediante Objetos de Directivas de Grupo (GPOs) que contienen configuraciones para usuarios o computadoras.

3.5 Open Directory

Open Directory es un concepto que sirve para referirse a dos entidades dentro de ambientes Apple.

Por un lado, Open Directory define a la arquitectura extensible de Servicios de Directorio para el sistema operativo Mac OS X (Figura 3-4), mediante la cual clientes y servidores Mac OS X pueden obtener información de usuarios y recursos de red desde una amplia variedad de servicios de directorio como pueden ser el servicio de LDAP de Mac OS X Server llamado Open Directory, Microsoft Active Directory, OpenLDAP, IBM Tivoli Directory Server, Novell eDirectory, Red Hat Directory Server y el servicio NIS de UNIX.

Por otro lado, Open Directory también es el nombre que recibe la implementación del servicio LDAP de Apple para sistemas Mac OS X y que es utilizada para almacenar y organizar objetos de usuario y de recursos de red en un Directorio.

[1] Domain Name System – Sistema de Nombres de Dominio

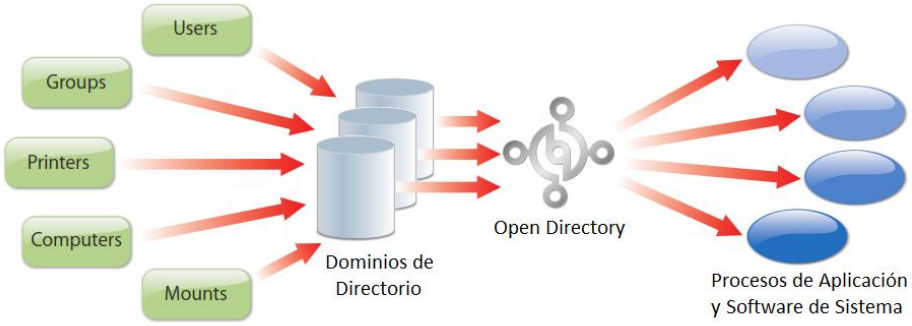

Figura 3-4 Servicios de Directorio y Open Directory

La implementación de Open Directory como Directorio LDAP está basada en OpenLDAP y fue implementada por primera vez en la versión 10.5 del sistema Mac OS X.

a. NetInfo

La primera implementación de Open Directory se presentó con la versión 10.2 de Mac OS X y estaba basada en un Dominio NetInfo y un servicio separado de administración de autenticación.

NetInfo es una base de datos de configuración que remplaza la mayoría de los archivos de configuración UNIX en los sistemas NeXTSTEP y posteriormente en Mac OS X 10.2 a 10.4, y entre la información que almacena se encuentra la siguiente:

- Alias Afpuser
- Alias
- Exports (comparticiones nfs)
- Grupos
- Equipos
- Puntos de montaje
- Redes
- Impresoras
- Protocolos
- RPCs
- Servicios
- Usuarios

Debido a que NetInfo no fue bien aceptado por la comunidad de usuarios y desarrolladores de sistemas UNIX, este no tuvo una amplia difusión y finalmente Apple lo sustituyó por LDAP.

b. Dominios y Servicios de Directorio en Open Directory

Open Directory provee de servicios de Directorio a los clientes y servidores Mac OS X actuando como un intermediario entre las aplicaciones y procesos del sistema que

necesitan leer o escribir información de usuarios y recursos de red, y uno o varios Dominios de Directorio que almacenan esa información.

El sistema operativo Mac OS X es un sistema UNIX certificado que está basado en NeXTSTEP, que a su vez está basado en FreeBSD y OpenBSD, pero a diferencia de estos sistemas UNIX que almacenan sus datos de administración en archivos de cofiguración, Mac OS X utiliza Open Directory para almacenar estos datos de administración.

c. Consolidación de Información

Tradicionalmente, los sistemas UNIX almacenan su información administrativa en un conjunto de archivos localizados en el directorio /etc, por lo que cada computadora UNIX requiere tener su propio conjunto de archivos para que los procesos que ejecute puedan leerlos cuando necesiten información administrativa. Por ejemplo, si un proceso requiere la contraseña de un usuario, este lee el archivo /etc/master.passwd y si requiere obtener información de la pertenencia de un usuario a un grupo, lee el archivo /etc/group (Figura 3-5).

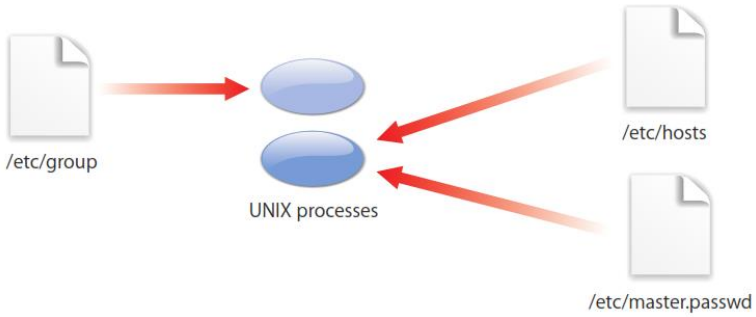

Figura 3-5 Almacenamiento de información en UNIX

En Mac OS X, Open Directory consolida la información administrativa mediante la implementación de un Directorio LDAP y fungiendo como intermediario con este u otros Directorios, por lo que los procesos que ejecuta un equipo Apple no requieren saber cómo y dónde está almacenada la información administrativa.

Por ejemplo, si un proceso requiere saber la pertenencia de un usuario a un grupo, este hace la solicitud a Open Directory para que él obtenga la información desde los Directorios que tenga configurados, aislando al proceso de los detalles sobre la forma en que está almacenada la información.

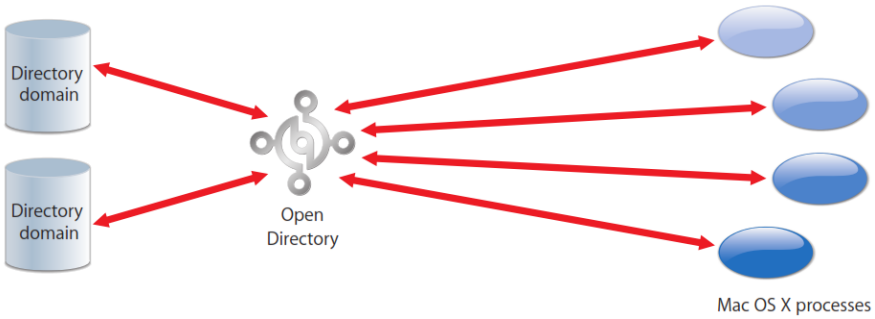

Figura 3-6 Consolidación de información con Open Directory

Una desventaja de los sistemas UNIX tradicionales, es que almacenan la información administrativa en archivos que solamente están disponibles en ese equipo, por lo que si un usuario requiere utilizar varios equipos, este deberá estar registrado en los archivos de configuración de cada uno de ellos, haciendo que las tareas administrativas se incrementen al tener que realizar cambios múltiples y con el consecuente riesgo de equivocaciones en la asignación de los permisos correctos.

En general, Open Directory consolida y distribuye la información para facilitar su acceso y mantenimiento, liberando a los administradores del pesado trabajo de mantener archivos independientes de configuración y permitiendo una administración centralizada de la información.

d. Dominio de Directorio Local

A partir de la versión 10.5 de Mac OS X, Apple sustituyó NetInfo por un directorio LDAP, por lo que cada computadora Mac tiene un Directorio de Dominio Local ejecutándose para administrar el almacenamiento de información administrativa, como la creación de cuentas de usuarios locales al equipo.

La información almacenada en un Directorio de Dominio Local, solamente está disponible para aplicaciones y procesos que se ejecuten en el equipo que aloja el Directorio, ya que esta información no puede ser compartida a otros equipos en la red.

Los Directorios de Dominio Locales están disponibles tanto en clientes como en servidores OS X y debido a que cada equipo tiene su propio Directorio, las cuentas de usuario deberán crearse en cada uno de ellos para poder compartir recursos en red, por ejemplo una carpeta compartida o SharePoint.

Al tenerse Directorios separados o independientes de manera local en cada equipo, se pierde la capacidad de Single-SignOn, sobre todo si se crea un usuario en varios directorios locales pero con contraseñas distintas (Figura 3-7).

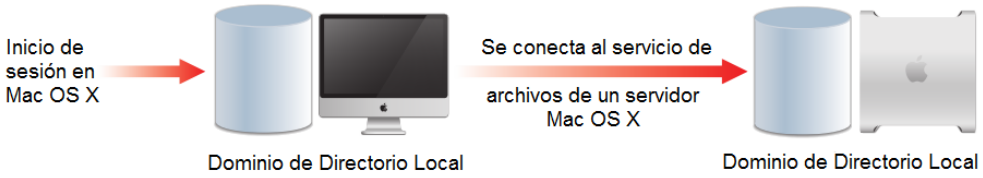

Figura 3-7 Dominio de Directorio Local

Es este caso, cuando un usuario inicia sesión en un cliente Mac OS X, este es autenticado por el Directorio Local y se le permitirá el acceso, pero una vez que ingrese al sistema solo tendrá acceso a recursos locales, a menos que se autentique a través de la red a otro equipo en el que también tenga creada una cuenta de usuario y enviando la contraseña apropiada para ese otro directorio local.

e. Dominio de Directorio Compartido

Para obtener el máximo poder de Open Directory, es necesario pasar de un Directorio local a un Directorio de Dominio Compartido que permita a varios equipos Mac OS X compartir información administrativa almacenada en un sistema central (
Figura 3-8).

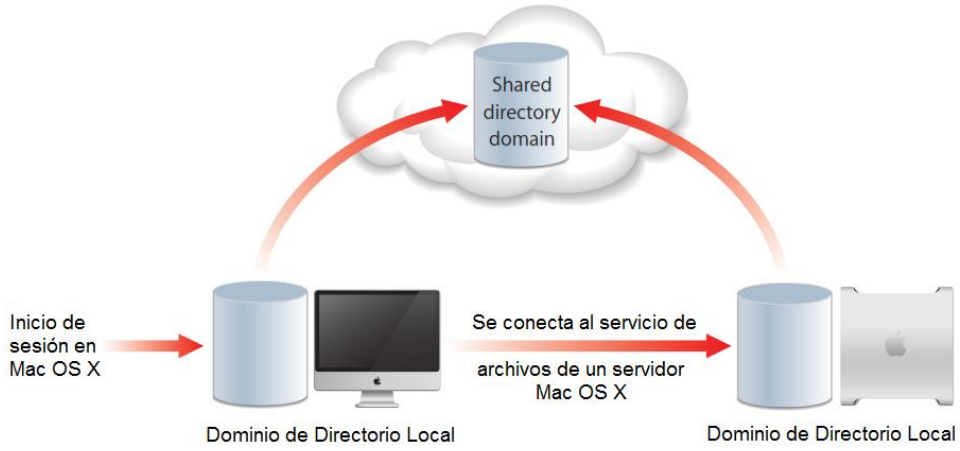

Figura 3-8 Dominio de Directorio Compartido

Cuando se configura un equipo para que utilice un dominio compartido, la información de este dominio compartido también estará disponible para las aplicaciones y software de sistema que se ejecute en ese equipo, por lo que si un usuario quiere iniciar sesión, Open Directory podrá buscar el registro del usuario en cualquier directorio compartido que tenga configurado el equipo para autenticarlo.

Debido a que los Dominios de Directorio almacenan información crítica para cualquier organización, como lo es la información de autenticación de usuarios, los Dominios Compartidos deben residir en servidores estrictamente protegidos y con características de hardware que garanticen una alta disponibilidad.

f. Dominios de Directorio Existentes

En la mayoría de las grandes organizaciones es común el uso de un Directorio para almacenar información de los usuarios, y de igual forma es común que estos directorios estén implementados en servidores Windows con Active Directory.

Open Directory es capaz de acceder a Dominios de Directorio de terceros como Open LDAP y Active Directory, y al mismo tiempo acceder a dominios Open Directory (Figura 3-9). A esta configuración se le conoce como el Triángulo Mágico.

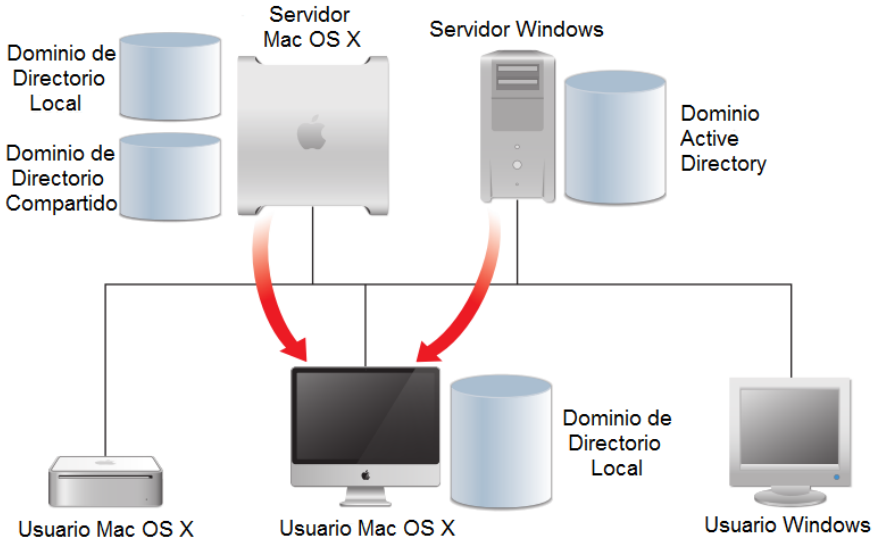

Figura 3-9 Integración con Dominios de Directorio de terceros

g. Roles de Open Directory

Cada servidor Mac OS X que participa en un ambiente Open Directory puede tener los siguientes roles:

1) Open Directory Master
   Este rol se aplica al servidor Open Directory primario que ejecuta la implementación de LDAP desarrollada por Apple y que almacena todas las configuraciones de la organización en un Directorio.

   Este rol es único y solamente un servidor puede tener este rol dentro de la organización, replicando su información a otros servidores Open Directory.

2) Open Directory Replica
   Este rol define a los servidores Open Directory que almacenan una copia completa de la configuración del servidor Open Directory Master y su función principal consiste en distribuir la carga y proporcionar redundancia del Directorio principal.

Las réplicas también son útiles para reducir el tráfico entre los enlaces de red a oficinas remotas, pues permiten que los clientes autentiquen de forma local, evitando el ruteo al sitio central.

En una infraestrucura Open Directory solamente puede existir un solo servidor Open Directory Master y este puede tener hasta 32 servidores Open Directory Replica conectados a él, y en el caso de que se requiera implementar más de 32 réplicas, cada uno de estos servidores réplica pueden tener otros 32 servidores conectados por su cuenta.

3) Conectado a un Servicio de Directorio
   Este rol implica que el servidor esté conectado como cliente a un sistema soportado por Open Directory, por lo que no replica ningún tipo de información de Kerberos o LDAP y no provee ningún servicio de autenticación central y solamente consumirá los servicios de otros servidores Open Directory Master o Replica para autenticar usuarios de forma local.

Capítulo 4
Análisis y metodología empleada

A lo largo de este capítulo se detalla el análisis realizado a las diferentes soluciones disponibles para la integración de Mac OS X con Active Directory, la selección de la mejor opción y el proceso de implementación.

4.1 Evaluación de Tecnologías

Durante el proceso de evaluación de las tecnologías disponibles para la integración de equipos Apple a la infraestructura de cómputo del Instituto de Ingeniería, se analizaron las distintas opciones que existen actualmente para integración del sistema operativo Mac OS X con Active Directory (Página 74 – Selección de la Solución), siendo este el punto principal a tomar en cuenta debido a que el Instituto ya cuenta con esta plataforma y ha alcanzado un nivel de madurez que la hace muy robusta.

Se analizaron las alternativas existentes para la administración de sistemas Mac OS X en ambientes empresariales que brindan la capacidad de tener una administración centralizada de estos equipos, tanto para distribuir configuraciones y aplicaciones a equipos en producción, como para aprovisionar equipos nuevos o que requieren ser reinstalados.

El análisis abarcó los complementos (plug-ins) nativos del sistema Mac OS X y soluciones de terceros como Centrify, PowerBroker y Quest (Tabla 4-1), y mostró que para una amplia mayoría de ambientes de red, la funcionalidad de los complementos nativos de Mac OS X son suficientes para proveer la funcionalidad necesaria para una integración exitosa, sin embargo, habrá escenarios en los que se requieran funcionalidades que estos no cubren y será necesario considerar una solución de terceros.

a. Complementos Nativos de Mac OS X

El sistema operativo Mac OS X incluye varios complementos que forman parte de su arquitectura extensible de Directorios llamada Open Directory, estos complementos son los que le permiten al sistema conectarse y hacer uso de los recursos almacenados en los distintos servicios de Directorio soportados.

Uno de los complementos incluidos es el “complemento LDAPv3”, el cual permite la integración con servicios de Directorio como Open Directory, OpenLDAP, IBM Tivoli Directory Server, Novell eDirectory y Red Hat Directory, pero este complemento no es compatible al cien por ciento con Microsoft Active Directory.

Esta incompatibilidad no está relacionada con la comunicación de fondo que se realiza mediante el estándar LDAP, sino que se refleja en atributos que no están disponibles en las versiones de Active Directory de Windows 2000 Server y Windows Server 2003, pues estas versiones no se apegaban completamente al estándar del RFC 2307 y fue hasta la versión de Windows Server 2003 R2 que Microsoft alineó los atributos de Active Directory a este estándar.

Debido a esta incompatibilidad, Apple diseñó un complemento especial para la integración de sus sistemas con Active Directory que es llamado el “complemento Active Directory”, pues aunque en versiones recientes de sistemas Microsoft, estos se apegan al RFC 2307, este complemento se encarga de operar como intermediario que hace una correlación de los atributos LDAP faltantes en versiones anteriores de Active Directory con atributos generados por el mismo complemento.

El complemento Active Directory también se encarga de hacer la traducción del formato de los valores de algunos de los atributos que no son compatibles entre sistemas Windows y Mac OS X, por ejemplo, si un usuario tiene definido un espacio de almacenamiento en red en el valor del atributo "Home Folder", en Windows la ruta se define en formato UNC[1] como **\\servidor\carpeta** y para que esta ubicación de red pueda ser utilizada en Mac OS X, el complemento de Active Directory se encarga de traducirlo como **smb://servidor/carpeta**.

Un factor importante a considerar es que los complementos de Open Directory, solamente resuelven la integración de la autenticación de usuarios, equipos y servicios, pero no proporcionan ninguna capacidad de administración centralizada mediante directivas. Para esto, es necesaria la implementación de un mecanismo de distribución de configuraciones que, para Mac OS X, Apple proporciona mediante una arquitectura basada en "Preferencias Administradas (Managed Preferences)".

Las Preferencias Administradas proveen a los administradores de las herramientas necesarias para controlar muchas de las funciones del sistema Mac OS X y están basadas en el sistema MCX de Apple; estas preferencias se editan con la herramienta "Workgroup Manager" y su distribución se hace básicamente con Open Directory, ya que las Preferencias Administradas utilizan LDAP y se almacenan como atributos dentro de los objetos de Open Directory (Figura 4-1).

En caso de que se deseen utilizar otros servicios de Directorio como Active Directory para almacenar y distribuir Preferencias Administradas a clientes Mac OS X, es necesario modificar o ampliar el esquema del Directorio. Este proceso de ampliación del esquema involucra la creación de clases de objeto y atributos especiales para Objetos Apple, y aunque estas modificaciones están plenamente identificadas, aún no existe un proceso automático para realizarlas y se requiere seguir un procedimiento manual de exportación e importación que implica los siguientes pasos.

1) Usar la herramienta de Microsoft "Active Directory Schema Analyzer" para comparar el esquema de Open Directory y Active Directory.
2) Seleccionar las clases de objeto y los atributos que existen en el esquema de Open Directory pero que no existen aún en Active Directory y exportarlos a un archivo LDIF.
3) Editar el archivo LDIF resultante para que sea posible importarlo a Active Directory.
4) Importar en Active Directory el archivo LDIF editado utilizando la herramienta de línea de comandos ldifde de Microsoft.

[1] Universal Naming Convention – Convención de Nombres Universal

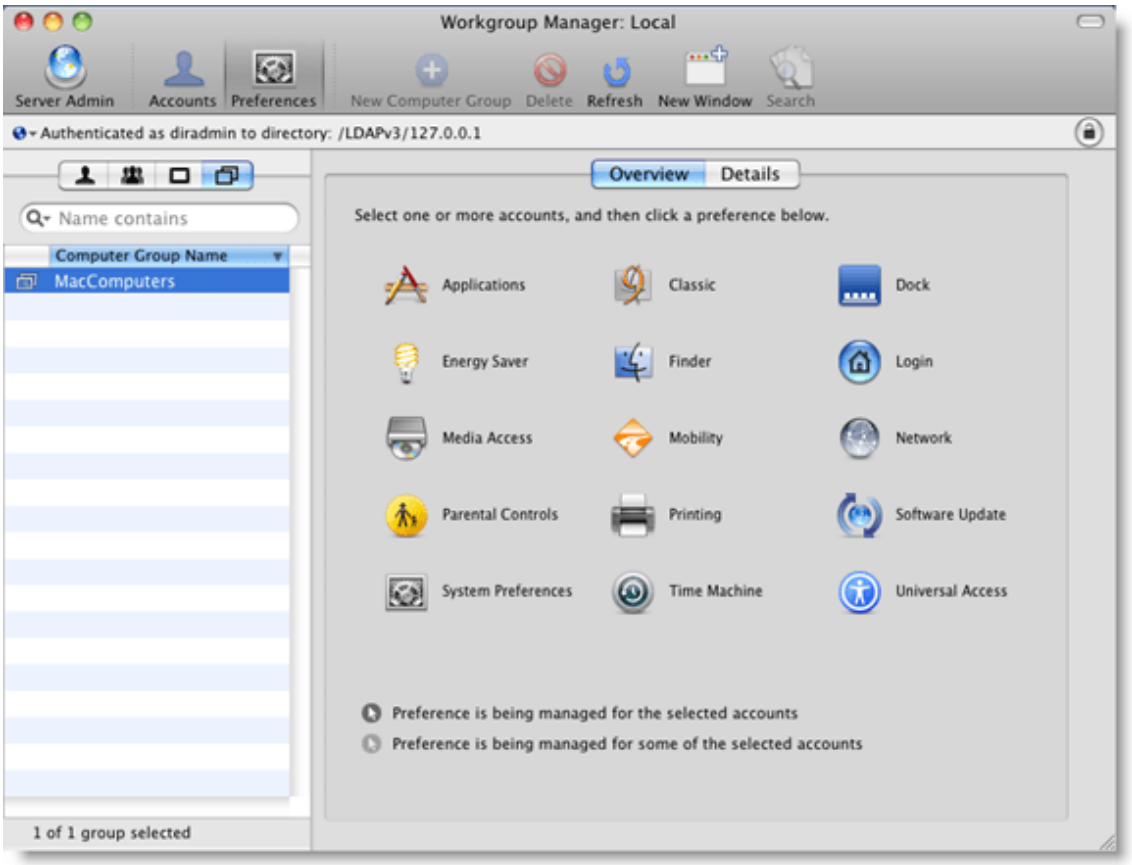

Figura 4-1 Herramienta Workgroup Manager de Apple

El proceso de ampliación o modificación del esquema de Active Directory es un tema delicado, pues una vez que se lleva a cabo, los cambios son replicados a todo el Bosque y revertir estas modificaciones implican una tarea complicada y de riesgo para la implementación del Directorio, por lo que muchas organizaciones optan por no realizar esta ampliación.

Como alternativa a la ampliación del esquema de Active Directory, se puede implementar un ambiente de Directorio Dual, en el que se utilicen de forma conjunta Active Directory y Open Directory, en un modelo que Apple llama el Triángulo Mágico o Triángulo Dorado.

La implementación de un ambiente de Directorio Dual, implica contar con dos Directorios, un Active Directory y un Open Directory completamente funcionales, a los cuales se unirán de forma simultánea los equipos cliente con sistema Mac OS X, por lo que estos realizarán consultas a los dos directorios de forma secuencial en el orden en que se hayan configurado en su ruta de búsqueda.

b. Centrify

Centrify DirectControl es una solución de integración de sistemas UNIX y Linux con Active Directory que incluye un componente de software para servidor que

complementa al Active Directory y un complemento o plug-in de Active Directory para los equipos cliente.

El componente de servidor extiende la funcionalidad de Active Directory sin que sea necesario extender su esquema para distribuir directivas de configuración a los clientes, mientras que el complemento de cliente utiliza la API[1] de los Servicios de Directorio de Mac OS X, por lo que se puede considerar que el complemento está al nivel de los complementos nativos de LDAPv3 y de Active Directory desarrollados por Apple.

La consola de administración de Centrify utiliza Zonas para agrupar computadoras UNIX, Linux y Mac OS X, estas Zonas permiten la distribución de directivas de configuración a los equipos cliente y se almacenan en un contenedor de Active Directory que se ubica en /Program Data/Centrify/Zones.

El complemento de cliente de Centrify provee las capacidades de inicio de sesión autenticando con Active Directory y aplica configuraciones definidas por GPOs desde los Controladores de Dominio, además de permitir el inicio de sesión con credenciales en caché. El proceso de instalación de este complemento es sencillo y durante este, se realizan las verificaciones necesarias para asegurar que está disponible el servidor con Centrify DirectControl y que la unión al Dominio será posible, por ejemplo verifica que exista un DC en el Site, que los relojes de los DCs y el cliente estén sincronizados y que funcione correctamente el servicio de DNS.

Del lado del servidor, Centrify se integra de forma muy robusta con las herramientas de administración de Windows Server, particularmente con la herramienta de gestión de usuarios Active Directory Users and Computers y con la Consola de Administración de Directivas de Grupo (GPMC[2]), haciendo la administración de equipos UNIX una tarea sencilla para cualquier administrador de redes Microsoft (Figura 4-2).

[1] Application Programming Interface
[2] Group Policy Management Console

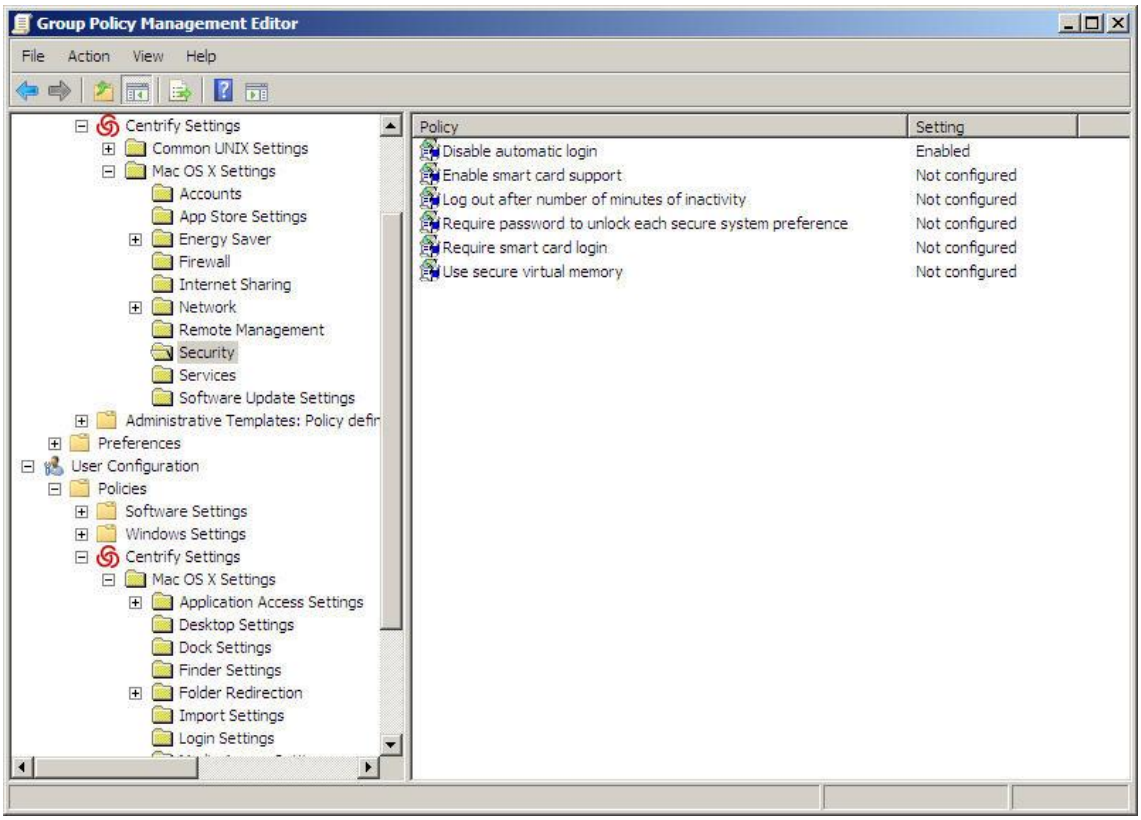

Figura 4-2 Plantilla Administrativa de Centrify para GPOs en Active Directory

c. BeyondTrust

PowerBroker Identity Services (antes Likewise) es una solución de BeyondTrust similar a la que provee Centrify, que permite la integración con Active Directory para sistemas UNIX y Linux mediante la instalación de dos elementos, uno en un servidor Windows y otro en los equipos cliente.

El componente de servidor de PowerBroker Identity Services se encarga de ampliar las características de las herramientas administrativas nativas de Active Directory en Windows como son Active Directory Users and Computers y la Consola de Administración de Directivas de Grupo, pues esta solución proporciona una alta integración con Group Policy (Figura 4-3).

Al igual que Centrify, PowerBroker Identity Services utiliza un concepto llamado Células para agrupar objetos de computadora y controlar su información. Estas Células están ligadas a Unidades Organizacionales (OUs), por lo que es posible asociar usuarios con estas Células modificando los atributos de la cuenta con la herramienta nativa de Active Directory Users and Computers.

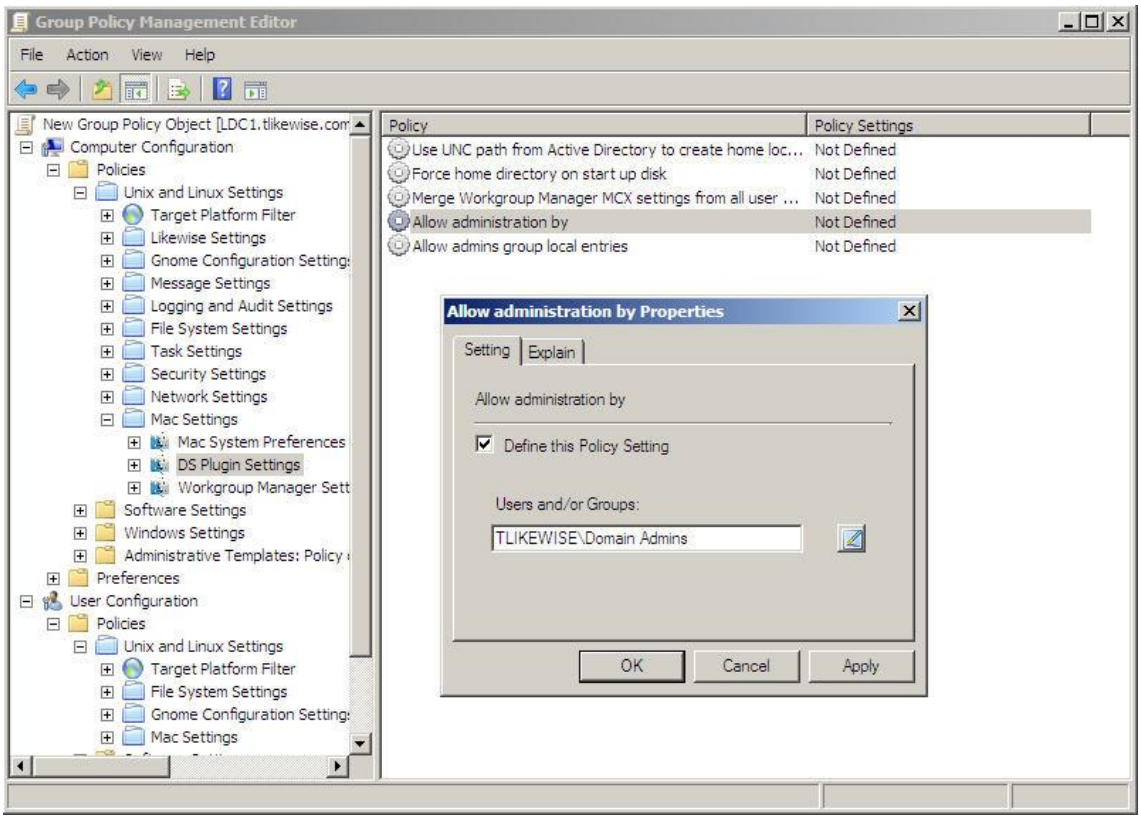

Figura 4-3 Directivas de PowerBroker Identity Services con Group Policy

Una característica interesante de PowerBroker Identity Services es que el componente de servidor puede actuar en un Modo Esquema o en un Modo Sin Esquema, y estos modos determinan la forma en que se hará la integración con Active Directory.

El Modo Esquema solamente puede ser utilizado si el Directorio está ejecutándose con el nivel de funcionalidad de Windows Server 2003 R2 o posterior, y no requiere que se hagan modificaciones al esquema de Active Directory.

Por otro lado, el Modo Sin Esquema está diseñado para trabajar con sistemas Windows 2000 Server y Windows Server 2003, que por diseño no se apegan completamente al RFC 2307. En este caso PowerBroker Identity Services ofrece dos opciones de implementación, una implica permitir a PowerBroker Identity Services que haga una ampliación al esquema de Active Directory, y la otra opción consiste en almacenar la información de usuario o grupo en los atributos “keywords” y “description” del Objeto usuario o computadora.

El componente de cliente de PowerBroker Identity Services puede instalarse a través de una aplicación gráfica de forma local en el equipo o a través de la red mediante SSH con una aplicación de línea de comandos.

El cliente de PowerBroker Identity Services se integra a la Utilidad de Directorios del sistema Mac OS X agregándose como un complemento más y por lo tanto se configura de forma similar al complemento nativo de Active Directory de Apple, proporcionando la capacidad de unir a Dominio el equipo y permitir la autenticación de usuarios durante el inicio de sesión en e equipo cliente. Además de la instalación de este complemento, PowerBroker Identity Services incluye una herramienta de migración de perfiles locales de usuario a perfiles de Directorio, por lo que se facilita la integración de equipos Mac OS X existentes a la infraestructura de Active Directory.

d. Quest

La solución de integración con Active Directory de Quest es llamada Authentication Services y es la evolución de Vintela Authentication Services o VAS que adquirieron tiempo atrás.

Authentication Services no utiliza Zonas o Células para agrupar objetos en Active Directory, por lo que la administración de la solución se simplifica al eliminar la complejidad de estos conceptos lógicos de agrupación.

Al igual que otras soluciones, Authentication Services requiere la instalación de un componente de servidor que se integra con las herramientas de administración de Active Directory (Figura 4-4) y que opera apegándose al RFC 2307 de LDAP, por lo que requiere que se extienda el esquema en caso de que no se esté utilizando Active Directory con un nivel de funcionalidad Windows Server 2003 R2 o posterior.

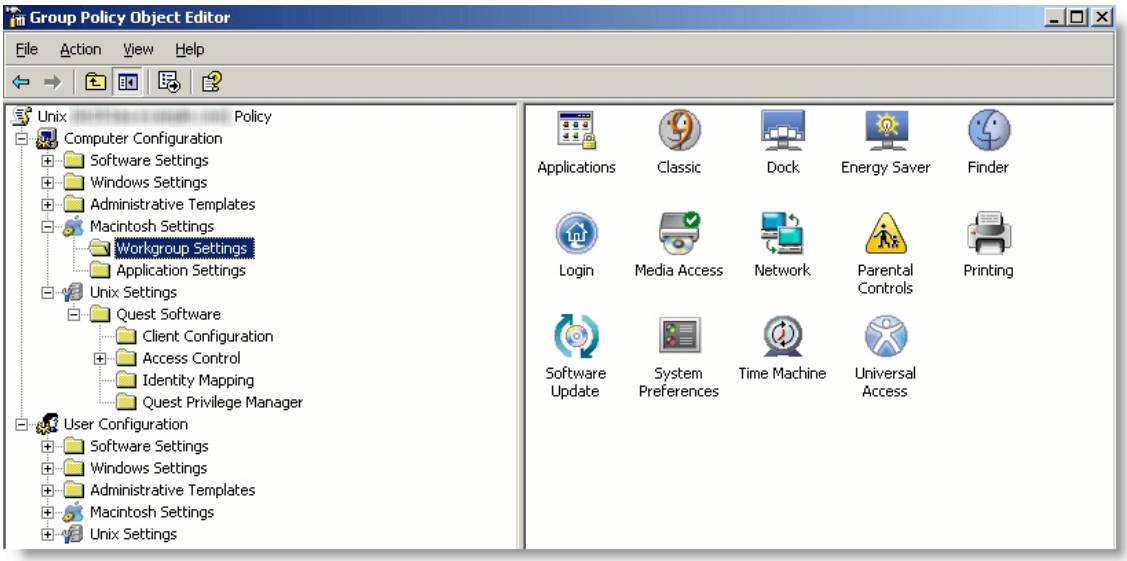

Figura 4-4 Administración de Preferencias mediante GPOs con Quest Authentication Services

A pesar de ofrecer una administración simplificada, Authentcation Services requiere que para iniciar sesión en un sistema UNIX, se habiliten las cuentas de los usuarios autorizados mediante la modificación del atributo "UNIX-Enabled" en su Objeto de Active Directory.

El componente de cliente para Mac OS X puede ser instalado localmente o por SSH a través de la red, además de que el proceso de instalación se encarga de unir el equipo al Dominio, haciendo las revisiones necesarias de cumplimiento de requisitos como el registro dinámico previo a DNS por parte del cliente, la sincronización de fecha y hora con los DCs y los permisos necesarios para la creación del Objeto en Active Directory.

4.2 Selección de la Solución

Una vez que evalué las tecnologías que pudiesen proveer la solución de integración de equipos Mac OS X en ambientes de red Microsoft para el Instituto de Ingeniería (Tabla 4-1), establecí que la elección de esta no debería estar solamente determinada por el costo de implementación, sino que se deberían considerar otros factores como la continuidad, el soporte del fabricante y la facilidad de administración; planteamiento que expuse al Coordinador de Sistemas de Cómputo, que al coincidir plenamente respaldó esta idea.

De acuerdo con los requerimientos observados durante la evaluación, se determinó que la infraestructura de Active Directory del Instituto cumple cabalmente con el RFC 2307 al ejecutarse sobre Windows Server 2012 R2 y por lo tanto se puede utilizar cualquiera de las soluciones para cubrir el requerimiento de autenticación de usuarios con Active Directory utilizando Kerberos.

Sin embargo, para cubrir el requerimiento de distribución de configuraciones de forma centralizada a través de la red, se analizaron las distintas técnicas que utilizan las soluciones evaluadas para almacenarlas y distribuirlas, y así determinar la opción que ofrezca una mejor compatibilidad, menor esfuerzo de implementación, soporte técnico confiable y un bajo costo total de propiedad a largo plazo.

Tabla 4-1 Comparativa de las soluciones evaluadas

Solución	Características
Complemento de Active Directory nativo de Mac OS X	• No se requiere hardware adicional • Se logra la integración con cualquier versión de Active Directory • Requiere la modificación del esquema de Active Directory • Soporta Kerberos • Es compatible con relaciones de confianza entre Dominios del Bosque • Soporta Firmado y Cifrado de paquetes
Directorio Dual (AD y OD)	• Requiere implementar un servidor Mac OS X con Open Directory • Se logra la integración con cualquier versión de Active Directory • No requiere modificar el esquema de Active Directory • Soporta Kerberos • Es compatible con relaciones de confianza entre Dominios del Bosque • Soporta Firmado y Cifrado de paquetes
Centrify Direct Control	• Se recomienda usar un servidor Windows dedicado • Se logra la integración solamente con Active Directory en Windows Server 2003 R2 o posterior • No requiere modificar el esquema de Active Directory • Soporta Kerberos • Es compatible con relaciones de confianza entre Dominios del Bosque • Soporta Firmado y Cifrado de paquetes

Solución	Características
PowerBroker Identity Services	• Se requiere un servidor Windows dedicado • Se logra la integración con cualquier versión de Active Directory • Requiere la modificación del esquema de Active Directory solamente para versiones previas a Windows Server 2003 R2 • Soporta Kerberos • Es compatible con relaciones de confianza entre Dominios del Bosque • Soporta Firmado y Cifrado de paquetes
Quest Authentication Services	• Se recomienda usar un servidor Windows dedicado • Se logra la integración solamente con Active Directory en Windows Server 2003 R2 o posterior • No requiere modificar el esquema de Active Directory • Soporta Kerberos • Es compatible con relaciones de confianza entre Dominios del Bosque • Soporta Firmado y Cifrado de paquetes

Un punto crucial que se alcanzó en el proyecto durante la selección de la solución a utilizar, fue la toma de decisión para elegir si se aceptaría la extensión del esquema de Active Directory, pues este es un elemento muy importante en la infraestructura del Instituto de Ingeniería y cualquier fallo puede causar daños serios a las operaciones académicas y administrativas diarias del Instituto.

El análisis del impacto que tendría realizar cambios al esquema del Directorio del Instituto junto con el análisis del comportamiento de la empresa Apple respecto al control de cambios que lleva de sus productos y soporte de compatibilidad para productos clasificados como en desuso, llevó a concluir que no se realizara la modificación al esquema de Active Directory.

Para esto se consideró que al hacer cambios al esquema del Directorio del Instituto, se harían modificaciones exclusivas para sistemas Mac OS X y no modificaciones genéricas que pudiesen ser aprovechadas por otros sistemas, además de que estos cambios no podrían revertirse fácilmente en caso de que se hiciera necesario modificarlos o prescindir de ellos en un futuro.

Además, se tomó en cuenta que la empresa Apple frecuentemente ha realizado cambios en su sistema operativo que no ofrecen compatibilidad con versiones anteriores, obligando a hacer actualizaciones que pudiesen generar problemas de convivencia con software o hardware, por lo que se concluyó que este era un riesgo que no se debería correr y esto hizo necesario considerar la opción de implementar una solución de Directorio Dual o de software de terceros.

El utilizar una solución de terceros fue una opción que en un principio se consideró viable, ya que las tres propuestas cubren los requisitos de implementación e integración básicos que estableció el Instituto de Ingeniería, pero esto implica introducir un tercer elemento a considerar en disputas de soporte técnico que pudiesen generar retrasos en la atención a los usuarios.

El Instituto de Ingeniería tiene lineamientos claros sobre el uso de sus equipos de cómputo, que básicamente debe apegarse a actividades estrictamente académicas, y sobre las configuraciones básicas de seguridad de estos, que deben ser homogéneas a

lo largo de la institución y se controlan de forma centralizada por la Coordinación de Sistemas de Cómputo.

Si bien estos lineamientos definen el uso y configuración de los equipos, en lo que se refiere a la instalación del tipo de sistema operativo, versión del mismo sistema operativo o las aplicaciones que deben tener los equipos de cómputo, el Instituto permite a los usuarios que ellos tomen la decisión de acuerdo a lo que mejor les convenga para la realización de sus actividades académicas, de acuerdo con la libertad académica a la que está acostumbrada la comunidad universitaria.

La libertad de decisión de los usuarios sobre la versión del sistema operativo que pueden elegir, complica el uso de una solución de terceros para la integración con Active Directory, pues normalmente después de la liberación de una versión nueva del sistema Mac OS X, los fabricantes de las soluciones de integración tardan bastante tiempo en ofrecer una actualización a su software que lo haga compatible con la nueva versión. Por lo que usuarios que actualicen su sistema operativo pueden llegar a perder la posibilidad de iniciar sesión en sus equipos y se incrementarían las solicitudes de soporte técnico a la CSC.

Para el caso de los servidores Windows con Active Directory la situación sería similar, pues aunque las actualizaciones de versión del sistema operativo se hacen mediante un proceso de evaluación e implementación controlado, una incompatibilidad del componente de integración puede llegar a retrasar las actividades de actualización hasta que el fabricante libere su actualización respectiva.

Estos puntos llevaron a descartar la utilización de las soluciones de terceros y finalmente se optó por la implementación de una infraestructura de Directorio Dual, que ofrece la ventaja de ser una solución que mantiene separados los procesos de actualización de cada sistema operativo pero sin descuidar la integración de Directorios.

Las actualizaciones de los sistemas Mac OS X cliente obtendrán una versión reciente de sus complementos de Directorio que mantienen su compatibilidad con Open Directory y Active Directory, sin necesidad de esperar a un tercero. Y las actualizaciones de los servidores Windows con Active Directory se podrán realizar de acuerdo con los tiempos planeados por el Instituto.

Otro elemento importante que llevó a descartar la implementación de una solución de terceros fue la inestabilidad de los grupos de soporte y la casi nula presencia que tienen en México, como es el caso de Centrify. A pesar de que Dell recientemente adquirió a Quest, el acercamiento que se tuvo con esta empresa reflejó poco conocimiento de los productos de Quest y un compromiso incierto para promover la solución; este caso se repite con BeyondTrust que ofrece su solución de integración a través de la compra que

hizo de la empresa Likewise, proceso en el que solamente conservaron 23 empleados[1]. Debido a estas situaciones, se decidió solamente considerar la solución nativa de Directorio Dual, en la que se puede contar con el soporte total de Microsoft y Apple.

4.3 Diseño de la Arquitectura

Para el diseño de la arquitectura de la solución se consideró que existen equipos Mac OS X cliente en las tres ubicaciones geográficas del Instituto y por lo tanto era necesario implementar al menos un servidor Mac OS X en las instalaciones de cada una de las sedes.

Estos servidores Mac OS X deberían formar la infraestructura de Open Directory del Instituto y por la criticidad de este nuevo servicio, estos deberían proveer el servicio de forma continua y sin interrupciones, por lo que se decidió implementar un servidor XServe con características altamente redundantes en el sitio central ubicado en Ciudad Universitaria (D.F.) y un servidor Mac Mini en cada una de las sedes remotas ubicadas en Juriquilla (Querétaro) y Sisal (Yucatán).

Tabla 4-2 Características del servidor de Ciudad Universitaria

Apple XServe	
Procesador	Doble procesador Quad-Core Intel Xeon de 2.26 GHz
RAM	24 GB DDR3 1066 MHz
Almacenamiento	1 Disco Duro de estado sólido de 128 GB 3 Discos Duros SCSI de 1 TB en RAID 5
Alimentación eléctrica	Dos fuentes redundantes de 127V

Tabla 4-3 Características del servidor de Juriquilla

Apple Mac Mini	
Procesador	1 Procesador Intel Core i7 de 2 GHz
RAM	16 GB DDR3 1333 MHz
Almacenamiento	1 Disco Duro de estado sólido de 256 GB 1 Disco Duro de SATA de 750 GB
Alimentación eléctrica	1 fuente de 127V

Tabla 4-4 Características del servidor de Sisal

Apple Mac Mini	
Procesador	1 Procesador Intel Core i7 de 2 GHz
RAM	16 GB DDR3 1333 MHz
Almacenamiento	1 Disco Duro de estado sólido de 256 GB 1 Disco Duro de SATA de 750 GB
Alimentación eléctrica	1 fuente de 127V

El servidor XServe de Ciudad Universitaria fue configurado como Open Directory Master y los servidores Mac Mini de Juriquilla y Sisal se configuraron como Open Directory Replicas para mantener la sincronización de la base de datos del Directorio y aislar las peticiones de autenticación de los clientes a su localidad geográfica.

[1] Fuente: http://www.geekwire.com/2012/emcs-isilon-division-buys-storage-software-company/

Cada uno de los servidores se configuraron para proporcionar una carpeta compartida en red para almacenar el software para el sistema Mac OS X que se distribuirá a los equipos cliente mediante la herramienta Apple Remote Desktop (ARD) que también fue instalada en cada uno de estos servidores para la administración remota de equipos cliente con fines de proporcionar soporte técnico y para la recolección de inventarios de hardware y software de los mismos clientes.

El principal motivo por el cual se implementó un servidor por localidad fue para separar los servicios de distribución de configuraciones y de distribución de software, de forma tal que no se saturaran los enlaces de comunicación a Internet. El hecho de que un cliente ubicado en Sisal Yucatán acuda al servidor Mac OS X para actualizar su configuración o autenticar un usuario, sería un proceso inaceptable por oponerse a las mejores prácticas de las Tecnologías de la Información.

El proceso de autenticación de los clientes se lleva a cabo directamente en los servidores de Active Directory mediante la resolución de nombres con DNS, proceso en el que se identifican a los servidores de autenticación con LDAP y los servidores de generación de llaves de Kerberos que dan el servicio a la sede correspondiente. De igual forma la distribución de políticas la realiza Open Directory a través del servidor local de la sede al identificar los rangos de direcciones IP asignados a los segmentos de red convenientes.

4.4 Implementación

El proceso de implementación lo dividí en dos etapas, una etapa involucró la instalación, configuración y puesta a punto de los servidores Mac OS X y la otra etapa radicó en la configuración de los equipos cliente para unirlos a un Dominio de la infraestructura de Active Directory del Instituto, y a su vez unirlos al Directorio formado por Open Directory, para lo cual desarrollé un script que permitiera la automatización de este proceso.

Durante este proceso se definieron las versiones de los sistemas operativos que se utilizarían en los servidores y los sistemas operativos que se soportarían en el lado de los clientes. Durante el inicio del proyecto se decidió trabajar con la versión 10.9 de Mac OS X “Mavericks” en los servidores, que es la última y más reciente versión liberada por Apple. Del lado de los clientes se dio por sentado que se tendría que trabajar con una serie de equipos con versiones heterogéneas del sistema operativo Mac OS X, y de acuerdo con un censo que se realizó previo a la implementación, se determinó que la versión del sistema operativo de los equipos que el Instituto de Ingeniería había adquirido en los últimos años comprendían las versiones 10.5 “Leopard”, 10.6 “Snow Leopard”, 10.7 “Lion”, 10.8 “Mountain Lion” y 10.9 “Mavericks”, por lo que solamente estas versiones fueron consideradas para las pruebas de compatibilidad de la solución.

4.5 Configuración de Servidores

La etapa de implementación de los servidores comenzó con la actualización del servidor XServe de Ciudad Universitaria, cambiando su sistema operativo que era Snow Leopard Server por la versión 10.9 "Mavericks". Lo mismo se aplicó a los dos servidores Mac Mini al actualizarlos de la versión 10.8 "Mountain Lion" a la versión 10.9 "Mavericks", con lo que se tuvo una plataforma homogénea sobre la cual se ejecutará Open Directory.

Una vez actualizados los servidores se realizó la configuración de cada uno de ellos, siguiendo el procedimiento descrito a continuación.

1. Debido a que la infraestructura actual de Active Directory utiliza Kerberos como método de autenticación, fue necesario sincronizar el reloj de los servidores Mac OS X con los Controladores de Dominio, que además de actuar como KDCs, proveen el servicio de sincronización de hora por medio del protocolo NTP.

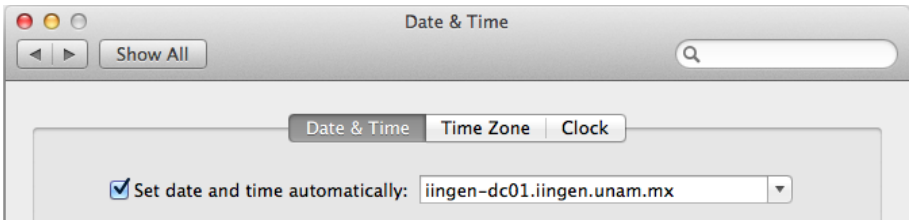

Figura 4-5 Sincronización de reloj en Mac OS X

2. El segundo paso consistió en realizar la unión de todos los servidores Mac OS X al dominio maestro IINGEN de Active Directory utilizando la herramienta "Utilidad de Directorios".

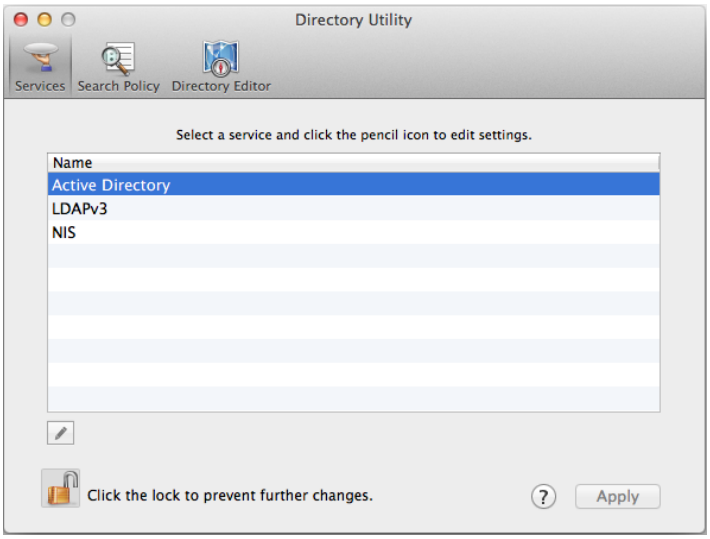

Figura 4-6 Utilidad de Directorio

Para esto se definieron los nombres *iingen-osx01*, *iingen-jq*-osx01 e *iingen-ss-osx01* para los servidores de CU, Juriquilla y Sisal respectivamente, y el Dominio

iingen.unam.mx como su Dominio de pertenencia; además se definió que los servidores deberían mantener cuentas móviles que mantengan un caché de inicio de sesión para poder ingresar al servidor con cuentas de dominio en caso de que se pierda la conectividad de red, y el uso de rutas UNC mediante el protocolo SMB para el acceso a la carpeta Home asignada a través de la red.

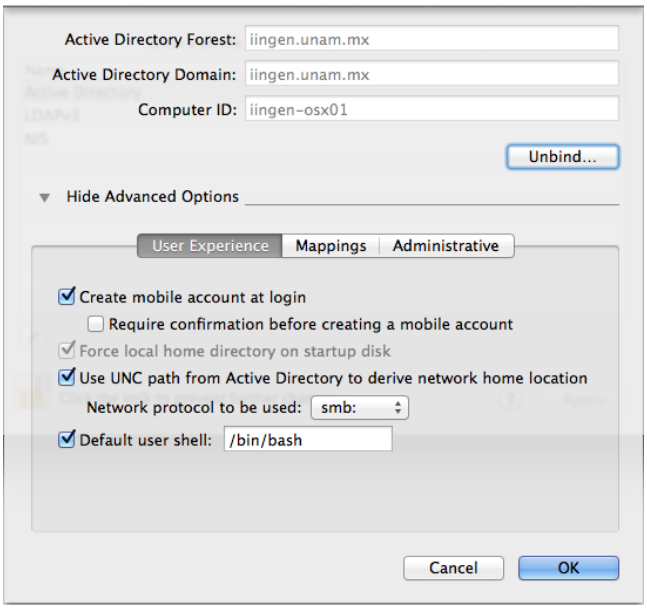

Figura 4-7 Configuración de cuentas móviles en Mac OS X

Finalmente, se configuraron los grupos "Domain Admins" y "Enterprise Admins" del Dominio IINGEN, con privilegios de administración sobre cada servidor, para que las cuentas que pertenezcan a ellos puedan administrar los servidores y así evitar la necesidad de volver a realizar esta configuración con la integración de nuevos miembros al equipo de trabajo de administración de servidores.

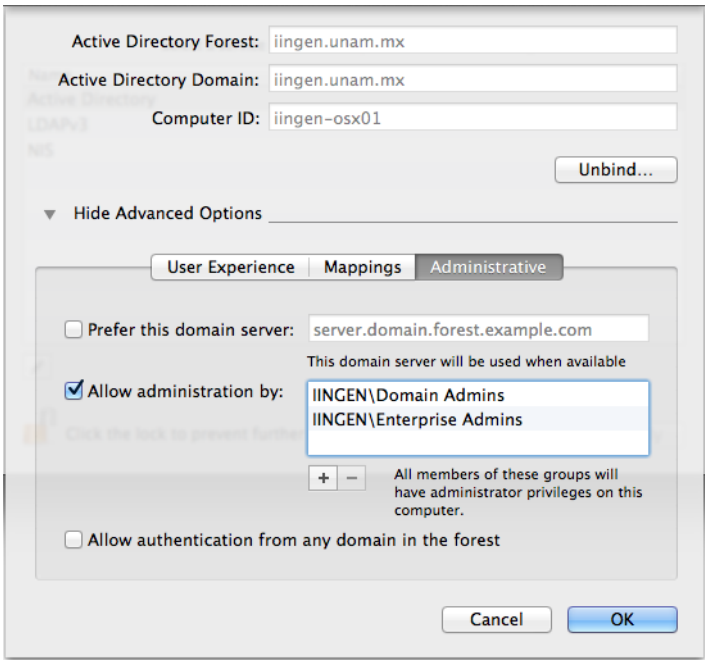

Figura 4-8 Integración de Administradores de Active Directory en Mac OS X

3. Se configuró el rol de Open Directory Master en el servidor de CU mediante la herramienta "Server".

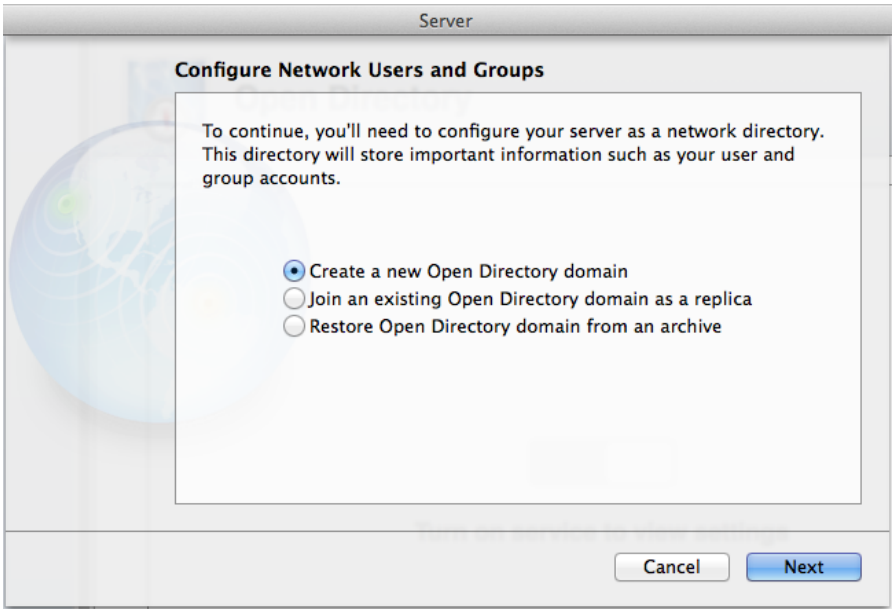

Figura 4-9 Creación de un nuevo Dominio Open Directory

Este procedimiento es extremadamente sencillo y solamente es necesario seguir el asistente de configuración que proporciona la interfaz gráfica, en la que se debe proporcionar el nombre de la cuenta que operará como administrador del

directorio, la contraseña de la cuenta, una dirección de correo electrónico de contacto para los usuarios del Directorio y el nombre de la organización.

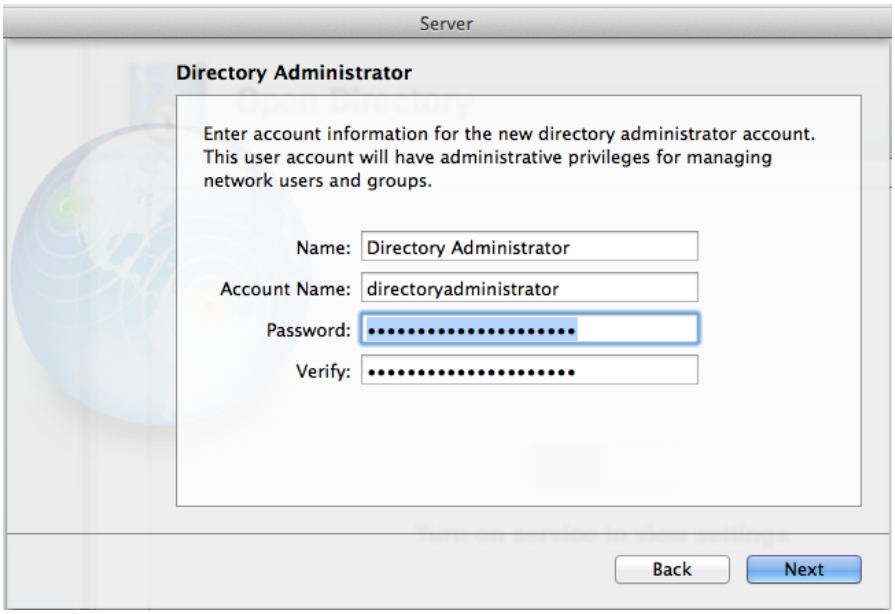

Figura 4-10 Creación de la cuenta de Administrador del Directorio

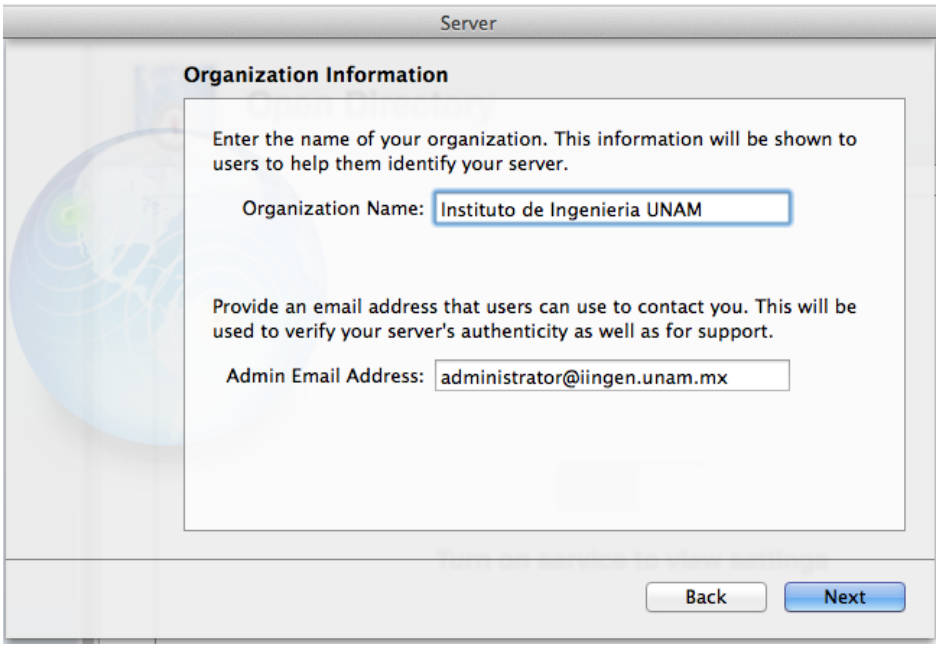

Figura 4-11 Asignación del nombre de la organización

4. Una vez creado el Directorio basado en Open Directory, se agregaron como servidores réplica los equipos Mac Mini de Juriquilla y Sisal

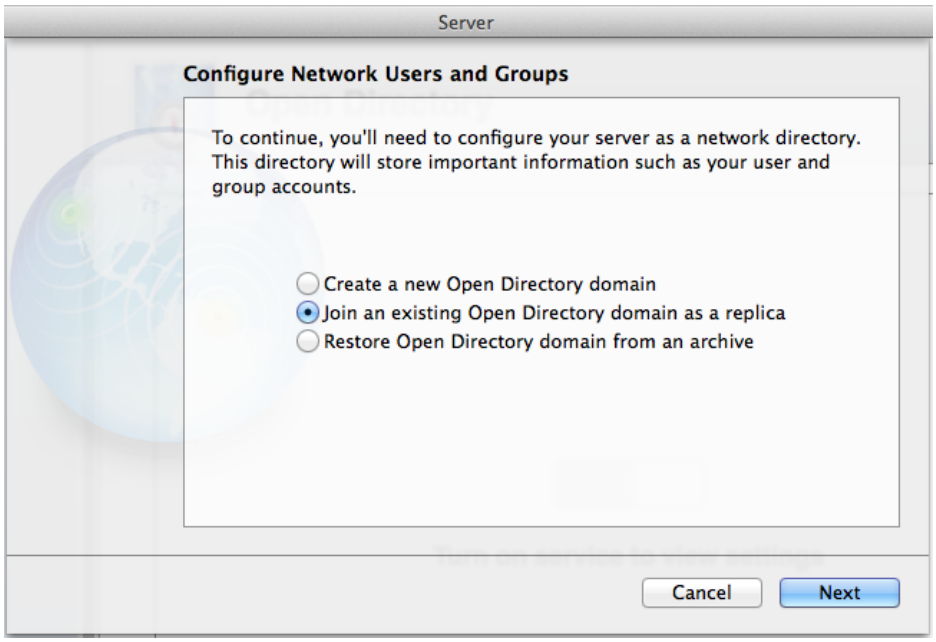

Figura 4-12 Creación de réplicas de Open Directory

El procedimiento de configuración del rol de Open Directory Replica es bastante sencillo y solamente se requiere que se defina el nombre del servidor que tiene el rol de Open Directory Master y las credenciales del administrador del Directorio.

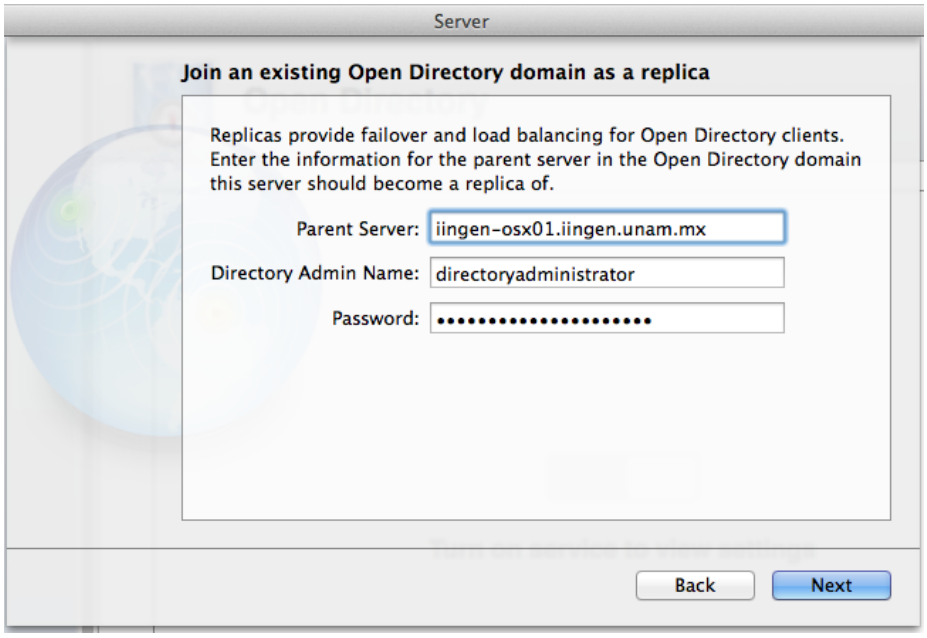

Figura 4-13 Definición del servidor "padre" para la réplica de Open Directory

4.6 Configuración de Clientes

La etapa de configuración de los equipos Mac OS X cliente, consistió en la elaboración de un plan de implementación que redujera el tiempo de ejecución y minimizara al máximo el riesgo de errores humanos al llevar a cabo las configuraciones.

Los elementos a configurar que se contemplaron en el plan de acción desarrollado fueron los siguientes.

1) Configurar la sincronización de la hora de los equipos cliente con los Controladores de Dominio de Active Directory, tal como lo hacen los equipos cliente con Windows.

2) Configurar el certificado digital de la Autoridad Certificadora del Instituto de Ingeniería en los clientes Mac OS X para que reconozcan como válidos los certificados emitidos por ella y así evitar el despliegue de alertas de seguridad a los usuarios.

3) Crear una cuenta local con privilegios de administración en los equipos cliente para realizar acciones administrativas en caso de que se pierda el enlace con los Directorios.

4) Configurar el cliente de Gestión Remota de Mac OS X en los clientes, para que puedan ser administrados con la herramienta Apple Remote Desktop de forma centralizada.

5) Cambiar el nombre de los equipos cliente para que se adapte a la convención de nombres de computadoras del Instituto de Ingeniería.

6) Unir al Dominio IINGEN los equipos cliente, pero siempre tomando en cuenta que el Objeto de computadora deberá crearse en la Unidad Organizacional que corresponda al área de trabajo del usuario final.

7) Habilitar el inicio de sesión único (Single Sign On) mediante la habilitación de Kerberos.

8) Enlazar los equipos cliente al Directorio de Open Directory recientemente generado, para que estos reciban configuraciones de forma centralizada.

9) Configurar la directiva de búsqueda del servicio de Directorios, colocando como primera opción de resolución a Active Directory.

Debido al gran número de cambios que se necesita hacer en los equipos cliente para que se cubran todos y cada uno de los puntos anteriores, se tomó la decisión de que esta configuración debería automatizarse para evitar errores u omisiones durante el

proceso y con esto se tendrá la certeza de que se tendrán equipos con una configuración consistente.

Para lograr la automatización, se consideró el lenguaje de programación de scripts nativo de Apple que es llamado AppleScript, el cual proporciona un lenguaje natural para la definición de procesos simples y la posibilidad de presentar elementos de la interfaz gráfica para interacción con el usuario, lo cual facilitó bastante la escritura del código y permitió controlar el orden de ejecución de cada uno de los módulos que cubren los requerimientos planteados en el proyecto.

AppleScript es un lenguaje estructurado que es interpretado y que se almacena en archivos de texto plano, pero también tiene la posibilidad de compilarse como aplicación nativa de Mac OS X, por lo que el código de automatización para la configuración de los equipos cliente pudo ser entregado al personal de soporte técnico de la CSC e incluso a usuarios finales de las sedes foráneas que no cuentan con personal de soporte suficiente, lo que les permitió que pudieran hacer la integración con los servicios de Directorio sin la necesidad de tener conocimientos avanzados en el tema.

En el código del Script de configuración se hace uso del lenguaje AppleScript, pero también se integra código del Shell Bash para operaciones de manejo de cadenas de texto y también se hace uso extenso de aplicaciones de línea de comando que sirven para configurar el sistema operativo.

Entre las aplicaciones de línea de comando que se utilizaron están las siguientes:

1) Systemsetup
   Herramienta de configuración para modificar algunos ajustes de computadora de las Preferencias del Sistema.

2) Dscl
   Herramienta que permite realizar operaciones sobre nodos del Directorio mediante comandos que permiten leer, crear y modificar datos del Servicio de Directorios.

3) Dsconfigad
   Herramienta que sirve para configurar el complemento de Active Directory y proporciona la misma funcionalidad de la Utilidad de Directorios del ambiente gráfico.

4) Dsconfigldap
   Herramienta que permite el agregado o remoción de configuraciones de servidores LDAP, incluyendo el enlace a estos Servicios de Directorio.

Conclusiones

En este apartado se hace un resumen del trabajo realizado y de cómo el Instituto de Ingeniería utiliza el resultado de este proyecto en su beneficio.

En la actualidad, el rápido desarrollo de nuevas tecnologías y la necesidad de mantener seguras las redes institucionales, ha ocasionado que sea imprescindible para cualquier organización el mantener un control estricto de los recursos de red y los dispositivos que tiene acceso a ellos.

Estos mecanismos de control incluyen la implementación de sistemas de autenticación avanzados y seguros que minimicen el riesgo de accesos no autorizados a información sensible que pudiese poner en riesgo la operaciones o reputación de la organización, y es por esto que se han desarrollado estándares que además de cubrir la necesidades antes mencionadas, permitan la interconexión en ambientes heterogéneos.

Uno de los sistemas básicos en toda red moderna es el Directorio, que comúnmente agrupa en forma objetos a todos los usuarios, equipos, impresoras y servicios de la organización, y al tratarse de un sistema crítico, es común que se utilicen estándares como LDAP para su almacenamiento y acceso, y Kerberos para asegurar la autenticación de los usuarios al acceder a los recursos de red.

Para el Instituto de Ingeniería ha sido de gran importancia el mantener un acercamiento agnóstico para el uso de tecnologías de la información y por lo tanto ha procurado mantener una infraestructura heterogénea que responda a las necesidades de los usuarios, pero sin retirar su atención en puntos clave como el control centralizado de los recursos para mantener los niveles necesarios de seguridad y funcionalidad.

El haber integrado de una forma simple y rápida los sistemas Mac OS X a su infraestructura, significó un nuevo reto para el Instituto, pero también corroboró el buen camino que se ha seguido durante los últimos dieciocho años, en los que se ha buscado siempre la facilidad de uso y acceso a los sistemas para toda la comunidad, mediante un Directorio que centraliza la autenticación y proporciona listas de usuarios y grupos para ser utilizados en las ACLs de los recursos compartidos, sitios Web, sistemas administrativos, sitios de colaboración, etc.

Los sistemas Mac OS X han significado de igual forma, un nuevo desafío para los usuarios del Instituto, que al encontrarlos integrados a la infraestructura de Directorio que conocen, ha facilitado su adopción y mejorado su experiencia con este sistema operativo, resultando en una transición menos complicada y un incremento de su productividad a corto plazo.

Para la Coordinación de Sistemas de Cómputo, este proyecto ha significado un avance en su capacidad para mantener la diversidad de sistemas que puede proteger bajo un mismo esquema de seguridad, y mediante el cual se agilizan las operaciones cotidianas de soporte al usuario por medio de la aplicación de un control estable de directivas que permiten la correcta toma de decisiones a nivel institucional.

Resultados y aportaciones

Presenta los resultados obtenidos después de la implantación de la solución, así como los beneficios obtenidos en el Instituto de Ingeniería, tanto para la Coordinación de Sistemas de Cómputo como para los usuarios.

La implementación de una arquitectura de Directorio Dual para la integración de equipos Mac OS X a la infraestructura de red del Instituto de Ingeniería de la UNAM, ha traído beneficios importantes a la comunidad, pues se ha logrado tener un nivel de integración completo con el mecanismo de autenticación central del Instituto, que se refleja en la capacidad de los usuarios de iniciar sesión en cualquier equipo autorizado con una única cuenta de usuario, eliminando la necesidad de solicitar una cuenta por equipo para su uso.

De igual forma se ha logrado que para los usuarios sea transparente el uso de recursos compartidos en red como carpetas e impresoras ubicadas en servidores especializados; de igual forma, se ha proporcionado un mecanismo estandarizado para crear recursos compartidos en equipos Mac OS X que pueden ser asegurados con listas de acceso o permisos que utilizan los grupos y usuarios del Directorio central del Instituto de Ingeniería.

Esto no solamente generó beneficios a los usuarios finales, sino también a los administradores de los recursos de red, que en este caso es el área que dirijo, al reducir la cantidad de solicitudes de soporte y eliminando la complejidad de administrar equipos distribuidos en distintas ubicaciones geográficas.

Adicionalmente, el Instituto de Ingeniería obtuvo una solución de bajo costo pero robusta al mismo tiempo, que le permite aprovechar al máximo sus recursos humanos y financieros para contribuir al alcance de su misión de contribuir al desarrollo del país y al bienestar de la sociedad a través de la investigación en ingeniería.

Finalmente, se logró la implementación de un sistema de administración centralizada que permite ofrecer un aprovisionamiento ágil de nuevos equipos a los usuarios y proporcionar soporte técnico de forma remota para reducir los tiempos de atención por parte del personal de la Coordinación de Sistemas de Cómputo, pero lo más importante es que sienta las bases para el desarrollo de una solución similar para sistemas Linux, cuya administración en el Instituto de Ingeniería se mantiene de forma local y aún no aprovecha los beneficios de una autenticación centralizada.

Apéndice

El apéndice de este trabajo incluye el código fuente en Apple Script que se desarrolló durante la ejecución de este proyecto, y que sirve para automatizar el proceso de unión a dominio de los equipos cliente con sistema operativo Mac OS X a la infraestructura de Active Directory del Instituto de Ingeniería de la UNAM.

El código fuente del Script para automatizar la configuración de los equipos cliente Mac OS X quedó escrito de la siguiente forma:

```
--Inicia Aplicacion
display dialog "Esta aplicación permite unir equipos Mac OS X a la infraestructura de Active Directory del Instituto de Ingeniería de la UNAM" with title "Instituto de Ingeniería UNAM" with icon 2 buttons {"Siguiente"}

--Obtiene Versión del Sistema Operativo
set versionOS to do shell script "defaults read /System/Library/CoreServices/SystemVersion.plist ProductVersion | awk '{split($0,num," & "\".\"); print num[1]\".\"num[2]}'" with administrator privileges

--Define variables para la creación de la cuenta de Administrador local
set localAdminRealName to "Administrador"
set localAdminRecordName to "administrador"
set localAdminPassword to "******** "

--Evita que se tome un UID que ya esté en uso
set ultimoUID to do shell script "dscl . -list /Users UniqueID | awk '$2 >= 500 {print $2}' | awk '$1 < 1000 {print $1}' | sort -ug | tail -1" with administrator privileges
if (ultimoUID is missing value) then
set ultimoUID to "500"
end if
set administradorExistente to do shell script "dscl . -list /Users UniqueID | awk '$2 >= 500 {print $1,$2}' | awk '$2 < 1000 {print $1,$2}' | awk '$1 ==" & space & "\"" & localAdminRecordName & "\"" & space & "{print $1}'" with administrator privileges
if administradorExistente is equal to localAdminRecordName then
set nuevoUID to do shell script "dscl . -list /Users UniqueID | awk '$2 >= 500 {print $1,$2}' | awk '$2 < 1000 {print $1,$2}' | awk '$1 ==" & space & "\"" & administradorExistente & "\"" & space & "{print $2}'" with administrator privileges
else
set nuevoUID to do shell script "expr " & ultimoUID & " + 1" with administrator privileges
end if

--Crea la cuenta de Administrador local
do shell script "dscl . -create /Users/" & localAdminRecordName with administrator privileges
do shell script "dscl . -create /Users/" & localAdminRecordName & space & "UserShell /bin/bash" with administrator privileges
do shell script "dscl . -create /Users/" & localAdminRecordName & space & "RealName " & localAdminRealName with administrator privileges
do shell script "dscl . -create /Users/" & localAdminRecordName & space & "UniqueID " & nuevoUID with administrator privileges
do shell script "dscl . -create /Users/" & localAdminRecordName & space & "PrimaryGroupID 20" with administrator privileges
do shell script "dscl . -create /Users/" & localAdminRecordName & space & "NFSHomeDirectory /Users/" & localAdminRecordName with administrator privileges
do shell script "dscl . -create /Users/" & localAdminRecordName & space & "Picture \"/Library/User Pictures/Animals/Eagle.tif\"" with administrator privileges
do shell script "dscl . -create /Users/" & localAdminRecordName & space & "dsAttrTypeNative:_writers_hint" & space & localAdminRecordName with administrator privileges
do shell script "dscl . -create /Users/" & localAdminRecordName & space & "dsAttrTypeNative:_writers_jpegphoto" & space & localAdminRecordName with administrator privileges
do shell script "dscl . -create /Users/" & localAdminRecordName & space & "dsAttrTypeNative:_writers_LinkedIdentity" & space & localAdminRecordName with administrator privileges
do shell script "dscl . -create /Users/" & localAdminRecordName & space & "dsAttrTypeNative:_writers_passwd" & space & localAdminRecordName with administrator privileges
do shell script "dscl . -create /Users/" & localAdminRecordName & space & "dsAttrTypeNative:_writers_picture" & space & localAdminRecordName with administrator privileges
do shell script "dscl . -create /Users/" & localAdminRecordName & space & "dsAttrTypeNative:_writers_realname" & space & localAdminRecordName with administrator privileges
do shell script "dscl . -create /Users/" & localAdminRecordName & space & "dsAttrTypeNative:_writers_UserCertificate" & space & localAdminRecordName with administrator privileges
do shell script "dscl . -create /Users/" & localAdminRecordName & space & "AuthenticationHint" & space & "Pregunta a LArellanoF" with administrator privileges
do shell script "dscl . -passwd /Users/" & localAdminRecordName & space & localAdminPassword with administrator privileges
do shell script "dscl . -append /Groups/admin GroupMembership " & localAdminRecordName with administrator privileges

--Habilita y Configura Gestión Remota para ARD
```

```
display dialog "Espere un momento" & return & return & "Preparando el equipo..." with title "Instituto de Ingeniería UNAM" with icon 2 buttons {"Cancelar"} giving up after 5
set usuariosARD to localAdminRecordName
do shell script "/System/Library/CoreServices/RemoteManagement/ARDAgent.app/Contents/Resources/kickstart -uninstall -settings" with administrator privileges
do shell script "/System/Library/CoreServices/RemoteManagement/ARDAgent.app/Contents/Resources/kickstart -activate" with administrator privileges
do shell script "/System/Library/CoreServices/RemoteManagement/ARDAgent.app/Contents/Resources/kickstart -configure -users " & usuariosARD & " -access -on -privs -all" with administrator privileges
do shell script "/System/Library/CoreServices/RemoteManagement/ARDAgent.app/Contents/Resources/kickstart -configure -allowAccessFor -specifiedUsers" with administrator privileges
do shell script "/System/Library/CoreServices/RemoteManagement/ARDAgent.app/Contents/Resources/kickstart -configure -clientopts -setmenuextra -menuextra no" with administrator privileges
do shell script "/System/Library/CoreServices/RemoteManagement/ARDAgent.app/Contents/Resources/kickstart -configure -clientopts -setreqperm -reqperm no" with administrator privileges
do shell script "/System/Library/CoreServices/RemoteManagement/ARDAgent.app/Contents/Resources/kickstart -configure -clientopts -setvnclegacy -vnclegacy no" with administrator privileges
do shell script "/System/Library/CoreServices/RemoteManagement/ARDAgent.app/Contents/Resources/kickstart -restart -agent -menu" with administrator privileges

--Instala Certificado de la Autoridad Certificadora IINGEN en el Llavero del Sistema
display dialog "Espere un momento" & return & return & "Instalando Certificado Digital..." with title "Instituto de Ingeniería UNAM" with icon 2 buttons {"Cancelar"} giving up after 5
do shell script "curl --get --output CAIINGEN.cer http://iingen-ca01.iingen.unam.mx/CertEnroll/CAIINGEN.cer" with administrator privileges
do shell script "security add-trusted-cert -d -r trustRoot -k \"/Library/Keychains/System.keychain\" \"CAIINGEN.cer\"" with administrator privileges
do shell script "rm CAIINGEN.cer" with administrator privileges

--Configura servidor de NTP y sincroniza la hora
do shell script "systemsetup -setnetworktimeserver iingen-dc01.iingen.unam.mx" with administrator privileges
do shell script "ntpdate -u" with administrator privileges

--Define la cuenta con privilegios para ingresar el equipo al Dominio de AD
set domainUser to "ADBinding"
set domainUserPassword to "********"

--Solicita información sobre el tipo de equipo
set TipoEquipo_dialog to choose from list {"Desktop", "Laptop"} with title "Instituto de Ingeniería UNAM" with prompt "Seleccione el Tipo de Equipo:" default items "" OK button name "Continuar" cancel button name "Cancelar" with multiple selections allowed
if TipoEquipo_dialog is false then return
set TipoEquipo to item 1 of TipoEquipo_dialog

--Solicita que se defina el nombre correcto del equipo antes de unirlo a Dominio
set currentName to (do shell script "scutil --get ComputerName")
set computerName to text returned of (display dialog "Verifique que el Nombre de Computadora sea el correcto" default answer currentName buttons {"Siguiente"} default button "Siguiente" with title "Instituto de Ingeniería UNAM")

--Renombra el equipo en caso de ser necesario
do shell script "systemsetup setcomputername " & computerName & space & "setlocalsubnetname " & computerName with administrator privileges

--Solicita información al usuario para definir la OU destino
set OU_dialog1 to choose from list {"Direccion", "Secretaria Academica", "Secretaria Administrativa", "Secretaria de Planeacion y Desarrollo Academico", "Secretaria Tecnica", "Subdireccion de Electromecanica", "Subdireccion de Estructuras y Geotecnia", "Subdireccion de Hidraulica y Ambiental", "Unidad de Gestión de Convenios y Contratos"} with title "Instituto de Ingeniería UNAM" with prompt "Seleccione la Unidad Organizacional del Equipo:" default items "" OK button name "Continuar" cancel button name "Cancelar" with multiple selections allowed
if OU_dialog1 is false then return
set OU_Principal to item 1 of OU_dialog1
if OU_Principal is equal to "Secretaria Academica" then
set OU_dialog2 to choose from list {"Unidad de Apoyo a Cuerpos Colegiados", "Unidad de Docencia y Formacion de Recursos Humanos", "Unidad de Gestion de Financiamiento", "Unidad de Informatica y Control Estadistico", "Unidad de Patentes y Transferencia Tecnologica", "Unidad de Promocion y Comunicacion", "Unidad de Servicios de Informacion"} with title "Instituto de Ingeniería UNAM" with prompt "Seleccione la Unidad a la que Pertenece el Equipo:" default items "" OK button name "Continuar" cancel button name "Cancelar" with multiple selections allowed
if OU_dialog2 is false then return
set OU_Secundaria to item 1 of OU_dialog2
```

```
else if OU_Principal is equal to "Secretaria Administrativa" then
set OU_dialog2 to choose from list {"Departamento de Bienes y Suministros", "Departamento de Contabilidad", "Departamento de Personal", "Departamento de Presupuesto"} with title "Instituto de Ingeniería UNAM" with prompt "Seleccione el Departamento al que Pertenece el Equipo:" default items "" OK button name "Continuar" cancel button name "Cancelar" with multiple selections allowed
if OU_dialog2 is false then return
set OU_Secundaria to item 1 of OU_dialog2
else if OU_Principal is equal to "Subdireccion de Electromecanica" then
set OU_dialog2 to choose from list {"Electrica y Computacion", "Ingenieria de Sistemas", "Instrumentacion", "Mecanica y Energia", "Sistemas de Computo"} with title "Instituto de Ingeniería UNAM" with prompt "Seleccione la Coordinación a la que Pertenece el Equipo:" default items "" OK button name "Continuar" cancel button name "Cancelar" with multiple selections allowed
if OU_dialog2 is false then return
set OU_Secundaria to item 1 of OU_dialog2
else if OU_Principal is equal to "Subdireccion de Estructuras y Geotecnia" then
set OU_dialog2 to choose from list {"Estructuras y Materiales", "Geotecnia", "Ingenieria Sismologica", "Mecanica Aplicada", "Sismologia e Instrumentacion Sismica"} with title "Instituto de Ingeniería UNAM" with prompt "Seleccione la Coordinación a la que Pertenece el Equipo:" default items "" OK button name "Continuar" cancel button name "Cancelar" with multiple selections allowed
if OU_dialog2 is false then return
set OU_Secundaria to item 1 of OU_dialog2
else if OU_Principal is equal to "Subdireccion de Hidraulica y Ambiental" then
set OU_dialog2 to choose from list {"Hidraulica", "Ingenieria Ambiental", "Ingenieria de Procesos Industriales y Ambientales", "Unidad Academica Juriquilla", "Unidad Academica Sisal"} with title "Instituto de Ingeniería UNAM" with prompt "Seleccione la Coordinación a la que Pertenece el Equipo:" default items "" OK button name "Continuar" cancel button name "Cancelar" with multiple selections allowed
if OU_dialog2 is false then return
set OU_Secundaria to item 1 of OU_dialog2
else
set OU_Secundaria to "Ninguna"
end if
if OU_Secundaria is equal to "Departamento de Contabilidad" then
set OU_dialog3 to choose from list {"Otros", "Area de Contabilidad"} with title "Instituto de Ingeniería UNAM" with prompt "Seleccione el Area a la que Pertenece el Equipo:" default items "" OK button name "Continuar" cancel button name "Cancelar" with multiple selections allowed
if OU_dialog3 is false then return
set OU_Area to item 1 of OU_dialog3
else if OU_Secundaria is equal to "Departamento de Presupuesto" then
set OU_dialog3 to choose from list {"Otros", "Area de Ingresos Extraordinarios"} with title "Instituto de Ingeniería UNAM" with prompt "Seleccione el Area a la que Pertenece el Equipo:" default items "" OK button name "Continuar" cancel button name "Cancelar" with multiple selections allowed
if OU_dialog3 is false then return
set OU_Area to item 1 of OU_dialog3
else if OU_Secundaria is equal to "Electrica y Computacion" then
set OU_dialog3 to choose from list {"Otros", "Coordinacion", "Ingenieria Linguistica"} with title "Instituto de Ingeniería UNAM" with prompt "Seleccione el Area a la que Pertenece el Equipo:" default items "" OK button name "Continuar" cancel button name "Cancelar" with multiple selections allowed
if OU_dialog3 is false then return
set OU_Area to item 1 of OU_dialog3
else if OU_Secundaria is equal to "Ingenieria de Sistemas" then
set OU_dialog3 to choose from list {"Ninguna", "Coordinacion", "Laboratorio de Transportes y Sistemas Territoriales"} with title "Instituto de Ingeniería UNAM" with prompt "Seleccione el Area a la que Pertenece el Equipo:" default items "" OK button name "Continuar" cancel button name "Cancelar" with multiple selections allowed
if OU_dialog3 is false then return
set OU_Area to item 1 of OU_dialog3
else if OU_Secundaria is equal to "Instrumentacion" then
set OU_dialog3 to choose from list {"Otros", "Coordinacion"} with title "Instituto de Ingeniería UNAM" with prompt "Seleccione el Area a la que Pertenece el Equipo:" default items "" OK button name "Continuar" cancel button name "Cancelar" with multiple selections allowed
if OU_dialog3 is false then return
set OU_Area to item 1 of OU_dialog3
else if OU_Secundaria is equal to "Mecanica y Energia" then
set OU_dialog3 to choose from list {"Otros", "Coordinacion", "Proyecto Impulsa"} with title "Instituto de Ingeniería UNAM" with prompt "Seleccione el Area a la que Pertenece el Equipo:" default items "" OK button name "Continuar" cancel button name "Cancelar" with multiple selections allowed
if OU_dialog3 is false then return
set OU_Area to item 1 of OU_dialog3
else if OU_Secundaria is equal to "Sistemas de Computo" then
```

```
set OU_dialog3 to choose from list {"Coordinacion", "Soporte Tecnico a PCs", "Servidores Windows Mac", "Sistemas Unix Linux", "Redes", "Sistemas Web", "Capacitacion", "Bases de Datos"} with title "Instituto de Ingeniería UNAM" with prompt "Seleccione el Area a la que Pertenece el Equipo:" default items "" OK button name "Continuar" cancel button name "Cancelar" with multiple selections allowed
if OU_dialog3 is false then return
set OU_Area to item 1 of OU_dialog3
else if OU_Secundaria is equal to "Estructuras y Materiales" then
set OU_dialog3 to choose from list {"Otros", "Coordinacion"} with title "Instituto de Ingeniería UNAM" with prompt "Seleccione el Area a la que Pertenece el Equipo:" default items "" OK button name "Continuar" cancel button name "Cancelar" with multiple selections allowed
if OU_dialog3 is false then return
set OU_Area to item 1 of OU_dialog3
else if OU_Secundaria is equal to "Geotecnia" then
set OU_dialog3 to choose from list {"Otros", "Coordinacion", "Laboratorio de Geoinformatica"} with title "Instituto de Ingeniería UNAM" with prompt "Seleccione el Area a la que Pertenece el Equipo:" default items "" OK button name "Continuar" cancel button name "Cancelar" with multiple selections allowed
if OU_dialog3 is false then return
set OU_Area to item 1 of OU_dialog3
else if OU_Secundaria is equal to "Ingenieria Sismologica" then
set OU_dialog3 to choose from list {"Otros", "Coordinacion"} with title "Instituto de Ingeniería UNAM" with prompt "Seleccione el Area a la que Pertenece el Equipo:" default items "" OK button name "Continuar" cancel button name "Cancelar" with multiple selections allowed
if OU_dialog3 is false then return
set OU_Area to item 1 of OU_dialog3
else if OU_Secundaria is equal to "Mecanica Aplicada" then
set OU_dialog3 to choose from list {"Otros", "Coordinacion"} with title "Instituto de Ingeniería UNAM" with prompt "Seleccione el Area a la que Pertenece el Equipo:" default items "" OK button name "Continuar" cancel button name "Cancelar" with multiple selections allowed
if OU_dialog3 is false then return
set OU_Area to item 1 of OU_dialog3
else if OU_Secundaria is equal to "Sismologia e Instrumentacion Sismica" then
set OU_dialog3 to choose from list {"Otros", "Coordinacion"} with title "Instituto de Ingeniería UNAM" with prompt "Seleccione el Area a la que Pertenece el Equipo:" default items "" OK button name "Continuar" cancel button name "Cancelar" with multiple selections allowed
if OU_dialog3 is false then return
set OU_Area to item 1 of OU_dialog3
else if OU_Secundaria is equal to "Hidraulica" then
set OU_dialog3 to choose from list {"Otros", "Coordinacion", "Costas y Puertos"} with title "Instituto de Ingeniería UNAM" with prompt "Seleccione el Area a la que Pertenece el Equipo:" default items "" OK button name "Continuar" cancel button name "Cancelar" with multiple selections allowed
if OU_dialog3 is false then return
set OU_Area to item 1 of OU_dialog3
else if OU_Secundaria is equal to "Ingenieria Ambiental" then
set OU_dialog3 to choose from list {"Otros", "Coordinacion", "Tratamiento y Reuso"} with title "Instituto de Ingeniería UNAM" with prompt "Seleccione el Area a la que Pertenece el Equipo:" default items "" OK button name "Continuar" cancel button name "Cancelar" with multiple selections allowed
if OU_dialog3 is false then return
set OU_Area to item 1 of OU_dialog3
else if OU_Secundaria is equal to "Ingenieria de Procesos Industriales y Ambientales" then
set OU_dialog3 to choose from list {"Otros", "Coordinacion"} with title "Instituto de Ingeniería UNAM" with prompt "Seleccione el Area a la que Pertenece el Equipo:" default items "" OK button name "Continuar" cancel button name "Cancelar" with multiple selections allowed
if OU_dialog3 is false then return
set OU_Area to item 1 of OU_dialog3
else if OU_Secundaria is equal to "Unidad Academica Juriquilla" then
set OU_dialog3 to choose from list {"Otros", "Coordinacion"} with title "Instituto de Ingeniería UNAM" with prompt "Seleccione el Area a la que Pertenece el Equipo:" default items "" OK button name "Continuar" cancel button name "Cancelar" with multiple selections allowed
if OU_dialog3 is false then return
set OU_Area to item 1 of OU_dialog3
else if OU_Secundaria is equal to "Unidad Academica Sisal" then
set OU_dialog3 to choose from list {"Otros", "Coordinacion"} with title "Instituto de Ingeniería UNAM" with prompt "Seleccione el Area a la que Pertenece el Equipo:" default items "" OK button name "Continuar" cancel button name "Cancelar" with multiple selections allowed
if OU_dialog3 is false then return
set OU_Area to item 1 of OU_dialog3
else
set OU_Area to "Ninguna"
end if
```

```
--Inicia la union a Dominio de AD
if OU_Area is equal to "Ninguna" then
if OU_Secundaria is equal to "Ninguna" then
do shell script "dsconfigad -f -a" & space & computerName & space & "-domain iingen.unam.mx -u" & space & domainUser & space & "-p" & space & domainUserPassword & space & "-lu" & space & localAdminRecordName & space & "-lp" & space & localAdminPassword & space & "-ou \"OU=" & TipoEquipo & "s MacOSX" & ",OU=" & OU_Principal & ",OU=Domain Computers,DC=iingen,DC=unam,DC=mx\"" with administrator privileges
else
do shell script "dsconfigad -f -a" & space & computerName & space & "-domain iingen.unam.mx -u" & space & domainUser & space & "-p" & space & domainUserPassword & space & "-lu" & space & localAdminRecordName & space & "-lp" & space & localAdminPassword & space & "-ou \"OU=" & TipoEquipo & "s MacOSX" & ",OU=" & OU_Secundaria & ",OU=" & OU_Principal & ",OU=Domain Computers,DC=iingen,DC=unam,DC=mx\"" with administrator privileges
end if
else
do shell script "dsconfigad -f -a" & space & computerName & space & "-domain iingen.unam.mx -u" & space & domainUser & space & "-p" & space & domainUserPassword & space & "-lu" & space & localAdminRecordName & space & "-lp" & space & localAdminPassword & space & "-ou \"OU=" & TipoEquipo & "s MacOSX" & ",OU=" & OU_Area & ",OU=" & OU_Secundaria & ",OU=" & OU_Principal & ",OU=Domain Computers,DC=iingen,DC=unam,DC=mx\"" with administrator privileges
end if
display dialog "Espere un momento" & return & return & "Uniendo el equipo a Dominio..." with title "Instituto de Ingeniería UNAM" with icon 2 buttons {"Cancelar"} giving up after 10

--Configuración del plugin de Active Directory

--1.User Experience
do shell script "dsconfigad -mobile enable -mobileconfirm disable -localhome enable -useuncpath enable -protocol smb -shell \"/bin/bash\"" with administrator privileges

--2.Mappings
do shell script "dsconfigad -nouid -nogid -noggid" with administrator privileges

--3.Administrative
do shell script "dsconfigad -nopreferred -groups \"IINGEN\\Enterprise Admins,IINGEN\\Domain Admins,IINGEN\\_CMP Soporte Tecnico a PCs,IINGEN\\_CMP Servidores Windows,IINGEN\\_CMP Infraestructura de Redes\" -alldomains enable -packetsign allow -packetencrypt allow -passinterval 14 -namespace domain" with administrator privileges

--Activa el Plugin de Active Directory
do shell script "defaults write /Library/Preferences/DirectoryService/DirectoryService 'Active Directory' Active" with administrator privileges

--Pausa para dar tiempo a DirectoryService para que aplique los cambios
display dialog "Espere un momento" & return & return & "Configurando las Opciones del Dominio..." with title "Instituto de Ingeniería UNAM" with icon 2 buttons {"Cancelar"} giving up after 30

--Configuración de la Política de Búsqueda de los Servicios de Directorio
if versionOS < 10.7 then
do shell script "dscl /Search -create / SearchPolicy CSPSearchPath" with administrator privileges
delay 5
do shell script "dscl /Search -append / CSPSearchPath \"/Active Directory/All Domains\"" with administrator privileges
do shell script "dscl /Search/Contacts -create / SearchPolicy CSPSearchPath" with administrator privileges
delay 5
do shell script "dscl /Search/Contacts -append / CSPSearchPath \"/Active Directory/All Domains\"" with administrator privileges
else if versionOS ≥ 10.7 then
do shell script "dscl /Search -create / SearchPolicy CSPSearchPath" with administrator privileges
delay 5
do shell script "dscl /Search -append / CSPSearchPath \"/Active Directory/IINGEN/All Domains\"" with administrator privileges
do shell script "dscl /Search/Contacts -create / SearchPolicy CSPSearchPath" with administrator privileges
delay 5
do shell script "dscl /Search/Contacts -append / CSPSearchPath \"/Active Directory/IINGEN/All Domains\"" with administrator privileges
else
delay 5
end if

--Habilita SSO con Kerberos
do shell script "dsconfigad -enableSSO" with administrator privileges
```

```
--Inicia la unión a Open Directory
set OpenDirectory to "iingen-osx01.iingen.unam.mx"
set DirectoryAdmin to "diradmin"
set DirectoryAdminPassword to "********"
do shell script "dsconfigldap -f –a" & space & OpenDirectory & space & "-c" & space & computerName & space & "-u" & space & DirectoryAdmin & space & "-p" & space & DirectoryAdminPassword & space & "-l" & space & localAdminRecordName & space & "-q" & space & localAdminPassword

--Muestra resultado de la Union a Dominio
display dialog (do shell script "dsconfigad -show" with administrator privileges)
```

Glosario

3DES
En criptografía, Triple DES se le llama al algoritmo que hace triple cifrado del DES y fue desarrollado por IBM en 1998. [14]

ACL
Access Control List o Lista de Control de Acceso, es un concepto de seguridad informática usado para fomentar la separación de privilegios. Es una forma de determinar los permisos de acceso apropiados a un determinado objeto. [14]

Active Directory
Es el término que usa Microsoft para referirse a su implementación de servicio de directorio en una red distribuida de computadores y que utiliza distintos protocolos como LDAP, DNS y Kerberos.

Es un Servicio de Directorio establecido en uno o varios servidores en donde se crean objetos como usuarios, equipos o grupos, con el objetivo de administrar los inicios de sesión en los equipos conectados a la red, así como también la administración de políticas en toda la red. [14]

AES
Advanced Encryption Standard o Estándar de Cifrado Avanzado, es un esquema de cifrado por bloques que tiene un tamaño de bloque fijo de 128 bits y tamaños de llave de 128, 192 o 256 bits. El cifrado fue desarrollado por dos criptólogos belgas, Joan Daemen y Vincent Rijmen, ambos estudiantes de la Katholieke Universiteit Leuven, y enviado en 1997 al proceso de selección de AES bajo el nombre "Rijndael". [14]

Apple
Es una empresa multinacional estadounidense con sede en Cupertino, Estados Unidos que diseña y produce equipos electrónicos y software. Entre sus productos de hardware más conocidos están las computadoras Macintosh, los reproductores de música iPod, los teléfonos iPhone y la tableta iPad. Entre el software de Apple se encuentran los sistemas operativos iOS y Mac OS X. [14]

Atributo
Es una especificación que define una propiedad de un Objeto, elemento o archivo. También puede referirse o establecer el valor específico para una instancia determinada de los mismos. [14]

Autenticación
Autenticación es el acto de establecimiento o confirmación de algo (o alguien) como auténtico. La autenticación de un objeto significa la confirmación de su procedencia, mientras que la autenticación de una persona a menudo consiste en verificar su identidad. [14]

Cifrado
En criptografía, el cifrado es un procedimiento que utiliza un algoritmo de cifrado con cierta clave secreta para transformar un mensaje de tal forma que sea incomprensible o, al menos, difícil de comprender a toda persona que no tenga la clave secreta (clave de descifrado) del algoritmo. Las claves de cifrado y de descifrado pueden ser iguales (criptografía simétrica) o no (criptografía asimétrica). [14]

CCITT
CCITT son las siglas de Comité Consultivo Internacional Telegráfico y Telefónico (Consultative Committee for International Telegraphy and Telephony - Comité Consultatif International Télégraphique et Téléphonique), antiguo nombre del comité de normalización de las telecomunicaciones dentro de la UIT (Unión Internacional de Telecomunicaciones) ahora conocido como UIT-T. [14]

Clase
Es una plantilla para la creación de objetos de datos según un modelo predefinido. Las clases se utilizan para representar entidades o conceptos, como los sustantivos en el lenguaje. Cada clase es un modelo que define un conjunto de variables -el estado, y métodos apropiados para operar con dichos datos -el comportamiento. Cada objeto creado a partir de la clase se denomina instancia de la clase. [14]

BYOD
Bring your Own Device o Trae tu Propio Dispositivo, es una política empresarial donde los empleados llevan sus propios dispositivos a su lugar de trabajo para tener acceso a recursos de la empresa tales como correos electrónicos, bases de datos y archivos en servidores así como datos y aplicaciones personales. [14]

DES
Data Encryption Standard o Estándar de Cifrado de Datos, es un algoritmo de cifrado escogido como un estándar FIPS en los Estados Unidos en 1976, y cuyo uso se ha propagado ampliamente por todo el mundo. El algoritmo fue controvertido al principio por contar con algunos elementos de diseño clasificados y una longitud de clave relativamente corta. [14]

DHCP
Dynamic Host Configuration Protocol o Protocolo de Configuración Dinámica de Equipos, es un protocolo de red que permite a los clientes de una red IP obtener sus parámetros de configuración automáticamente. Se trata de un protocolo de tipo cliente/servidor en el que generalmente un servidor posee una lista de direcciones IP

dinámicas y las va asignando a los clientes conforme éstas van quedando libres, sabiendo en todo momento quién ha estado en posesión de esa IP, cuánto tiempo la ha tenido y a quién se la ha asignado después. [14]

Directorio
Un directorio es un conjunto de objetos con atributos organizados en una manera lógica y jerárquica. [14]

DNS
Domain Name System o Sistema de Nombres de Dominio, es un sistema de nomenclatura jerárquica para computadoras, servicios o cualquier recurso conectado a Internet o a una red privada. Este sistema asocia información variada con nombres de dominios asignado a cada uno de los participantes. Su función más importante, es traducir (resolver) nombres inteligibles para las personas en identificadores binarios asociados con los equipos conectados a la red, esto con el propósito de poder localizar y direccionar estos equipos mundialmente.

El servidor DNS utiliza una base de datos distribuida y jerárquica que almacena información asociada a nombres de dominio en redes como Internet. Aunque como base de datos el DNS es capaz de asociar diferentes tipos de información a cada nombre, los usos más comunes son la asignación de nombres de dominio a direcciones IP y la localización de los servidores de correo electrónico de cada dominio. [14]

Dominio
Es una red de identificación asociada a un grupo de dispositivos o equipos conectados a la red. [14]

IETF
Internet Engineering Task Force o Grupo de Trabajo de Ingeniería de Internet, es una organización internacional abierta de normalización, que tiene como objetivos el contribuir a la ingeniería de Internet, actuando en diversas áreas, como transporte, encaminamiento y seguridad. Fue creada en Estados Unidos en 1986 y es mundialmente conocida por ser la entidad que regula las propuestas y los estándares de Internet, conocidos como RFC. [14]

ISO
International Standards Organization u Organización Internacional de Normalización, es el organismo encargado de promover el desarrollo de normas internacionales de fabricación (tanto de productos como de servicios), comercio y comunicación para todas las ramas industriales a excepción de la eléctrica y la electrónica. Su función principal es la de buscar la estandarización de normas de productos y seguridad para las empresas u organizaciones (públicas o privadas) a nivel internacional. [14]

ITU-T
Sector de Normalización de las Telecomunicaciones de la UIT (UIT-T), con sede en Ginebra Suiza, es el órgano permanente de la Unión Internacional de Telecomunicaciones (UIT) que estudia los aspectos técnicos, de explotación y tarifarios, y publica normativas sobre los mismos, con vista a la normalización de las telecomunicaciones a nivel mundial. Fue conocido hasta 1992 como Comité Consultivo Internacional Telefónico y Telegráfico (CCITT). [14]

Kerberos
Kerberos es un protocolo de autenticación de redes informáticas creado por el MIT que permite a dos ordenadores en una red insegura demostrar su identidad mutuamente de manera segura. Sus diseñadores se concentraron primeramente en un modelo de cliente-servidor, y brinda autenticación mutua: tanto cliente como servidor verifican la identidad uno del otro.

Kerberos se basa en criptografía de clave simétrica y requiere un tercero de confianza y sus mensajes de autenticación están protegidos para evitar eavesdropping y ataques de Replay. [14]

LDAP
Lightweight Directory Access Protocol o Protocolo Ligero de Acceso a Directorios, hace referencia a un protocolo a nivel de aplicación que permite el acceso a un servicio de directorio ordenado y distribuido para buscar diversa información en un entorno de red. LDAP también se considera una base de datos a la que pueden realizarse consultas, aunque su sistema de almacenamiento puede ser diferente. [14]

Linux
Linux es un sistema operativo libre, basado en Unix. Es uno de los principales ejemplos de software libre y de código abierto que está licenciado bajo GPL y es desarrollado por colaboradores de todo el mundo. [14]

Mac OS X
Es un sistema operativo basado en Unix, desarrollado, comercializado y vendido por Apple Inc. Ha sido incluido en su gama de computadoras Macintosh desde el año de 2002. [14]

Microsoft
Es una empresa multinacional de origen estadounidense, fundada el 4 de abril de 1975 por Bill Gates y Paul Allen. Dedicada al sector del software y el hardware, con sede en Redmond, Washington, Estados Unidos.

Desarrolla, fabrica, licencia y produce software y equipos electrónicos, siendo sus productos más usados el sistema operativo Windows y la suite Microsoft Office, los cuales tienen una importante posición entre las computadoras personales con una participación de mercado cercana al 90% [14]

Objeto
Es la unidad básica de información que se almacena en un Directorio y su función es representar elementos de la vida real como personas, servidores, computadoras, impresoras, organizaciones, etc.

Un objeto está formado por un conjunto de atributos que contienen información sobre él y cada atributo puede tener uno o más valores pero un solo tipo de información. [14]

Open Directory
Es la implementación del modelo de servicio de directorio LDAP desarrollada por Apple.

Open Directory describe un dominio de directorio LDAPv3 y su correspondiente modelo de autenticación compuesto por Apple Password Server y Kerberos 5 mediante un sistema modular de servicios de directorio, aunque también describe el framework completo de servicios de directorio usado por Mac OS X y Mac OS X Server describiendo el rol de estos sistemas cuando se conectan a servicios de directorio existentes. [14]

Open LDAP
Es una implementación libre y de código abierto del protocolo LDAP desarrollada por el proyecto OpenLDAP. [14]

OSI
El modelo de interconexión de sistemas abiertos (ISO/IEC 7498-1), también llamado OSI (en inglés, Open System Interconnection 'interconexión de sistemas abiertos') es el modelo de red descriptivo, que fue creado por la Organización Internacional para la Estandarización (ISO) en el año 1980.1 Es un marco de referencia para la definición de arquitecturas en la interconexión de los sistemas de comunicaciones. [14]

Plug-in
También llamado complemento, es una aplicación que se relaciona con otra para aportarle una función nueva y generalmente muy específica. Esta aplicación adicional es ejecutada por la aplicación principal e interactúan por medio de una API. También se conoce como add-on, añadido, conector o extensión. [14]

RC4
Dentro de la criptografía RC4 o ARC4 es el sistema de cifrado de flujo Stream cipher más utilizado y se usa en algunos de los protocolos más populares como Transport Layer Security (TLS/SSL) (para proteger el tráfico de Internet) y Wired Equivalent Privacy (WEP) (para añadir seguridad en las redes inalámbricas). RC4 fue excluido enseguida de los estándares de alta seguridad por los criptógrafos y algunos modos de usar el algoritmo de criptografía RC4 lo han llevado a ser un sistema de criptografía muy inseguro, incluyendo su uso WEP. No está recomendado su uso en los nuevos sistemas,

sin embargo, algunos sistemas basados en RC4 son lo suficientemente seguros para un uso común. [14]

RFC
Request for Comments o Petición de Comentarios, son una serie de publicaciones del Internet Engineering Task Force (IETF) que describen diversos aspectos del funcionamiento de Internet y otras redes de computadoras, como protocolos, procedimientos, etc. y comentarios e ideas sobre estos. Cada RFC constituye un monográfico o memorando que ingenieros o expertos en la materia han hecho llegar al IETF, para que éste sea valorado por el resto de la comunidad. [14]

SQL
Structured Query Language o Lenguaje de Consulta Estructurado, es un lenguaje declarativo de acceso a bases de datos relacionales que permite especificar diversos tipos de operaciones en ellas. Una de sus características es el manejo del álgebra y el cálculo relacional que permiten efectuar consultas con el fin de recuperar de forma sencilla información de interés de bases de datos, así como hacer cambios en ellas. [14]

TI
Tecnologías de la información, es un concepto que tiene dos significados. En el uso común se usa a menudo para referirse a cualquier forma de hacer cómputo, y en el uso especializado, se refiere a la preparación para satisfacer las necesidades de tecnologías en cómputo y comunicación de cualquier tipo de organización requiriendo una base muy sólida de la aplicación de los conceptos fundamentales de áreas como las ciencias de la computación, así como de gestión y habilidades del personal. [14]

UNIX
Es un sistema operativo portable, multitarea y multiusuario, desarrollado en 1969 por un grupo de empleados de los laboratorios Bell de AT&T, entre los que figuran Ken Thompson, Dennis Ritchie y Douglas McIlroy. [14]

Windows
Es un sistema operativo gráfico desarrollado y vendido por Microsoft, introducido el 20 de noviembre de 1985 como un Shell gráfico para MS-DOS. Ha llegado a dominar el mercado mundial de las computadoras personales con cerca del 90% de participación. [14]

X.500
X.500 es un conjunto de estándares de redes de ordenadores de la ITU-T sobre servicios de directorio. El estándar se desarrolló conjuntamente con la ISO como parte del Modelo de interconexión de sistemas abiertos, para usarlo como soporte del correo electrónico X.400. [14]

Bibliografía

[1] Steven Tuttle, Ami Ehlenberger, Ramakrishna Gorthi, Jay Leiserson, Richard Macbeth, Nathan Owen, Sunil Ranahandola, Michael Storrs y Chunhui Yang, 2004. *UNDERSTANDING LDAP – DESIGN AND IMPLEMENTATION*. 2ª edición. Estados Unidos de América: IBM Redbooks

[2] Laura E. Hunter, 2005. *ACTIVE DIRECTORY FIELD GUIDE*. Estados Unidos de América: Apress

[3] Jason Garman, 2003. *KERBEROS: THE DEFINITIVE GUIDE*. Estados Unidos de América: O'Reilly & Associates

[4] Charles S. Edge Jr., Chris Barker y Ehren Schwiebert, 2010. *BEGINNING MAC OS X SNOW LEOPARD SERVER FROM SOLO INSTALL TO ENTERPRISE INTEGRATION*. Estados Unidos de América: Apress

[5] Apple, 2009. *MAC OS X SERVER OPEN DIRECTORY ADMINISTRATION, VERSION 10.6 SNOW LEOPARD*. Estados Unidos de América: Apple

[6] Arek Dreyer, Ben Greisler, 2010. *MAC OS X SERVER ESSENTIALS V10.6*. Estados Unidos de América: Peachpit

[7] Arek Dreyer, Ben Greisler, 2010. *MAC OS X DIRECTORY SERVICES V10.6*. Estados Unidos de América: Peachpit

[8] Charles S. Edge Jr., Beau Hunter y Zack Smith, 2009. *ENTERPRISE MAC ADMINISTRATOR'S GUIDE*. Estados Unidos de América: Apress

[9] Dan Holme, Nelson Ruest y Danielle Ruest, 2008. CONFIGURING WINDOWS SERVER 2008 ACTIVE DIRECTORY. Estados Unidos de América: Microsoft Press

[10] Mike Bombich, 2006. *LEVERAGING ACTIVE DIRECTORY ON MAC OS X*. [pdf]. Disponible en: < http://www.static.afp548.com/mactips/activedir.html >

[11] Trapti Ozha, 2013. *KERBEROS: AN AUTHENTICATION PROTOCOL*. International Journal of Computer Technology and Applications, [online] Disponible en: <http://www.ijcta.com/vol4issue2-page2.php>

[12] OCLC, *X.500 AND LDAP*. [pdf]. Disponible en: <http://www.collectionscanada.gc.ca/iso/ill/document/ill_directory/X_500and LDAP.pdf>

[13] Eric B. Rux, 2011. Comparative Review: Mac-to-AD Integration Solutions. WindowsITPro, [online] Disponible en: http://windowsitpro.com/active-directory/comparative-review-mac-ad-integration-solutions

[14] Fundación Wikimedia, 2014, WIKIPEDIA, [online] Disponible en: http://www.wikipedia.org/