UNIVERSIDAD TÉCNICA DE COTOPAXI

FACULTAD DE CIENCIAS DE LA INGENIERÍA Y APLICADAS

CARRERA DE INGENIERÍA EN INFORMÁTICA Y SISTEMAS COMPUTACIONALES

PROYECTO DE INVESTIGACIÓN

IMPLEMENTACIÓN Y ADMINISTRACIÓN DE UN SERVIDOR DE DOMINIO, MEDIANTE SECURITY ACCOUNT MANAGER, PARA CENTRALIZAR LOS RECURSOS, SERVICIOS DE LAS TIC´S, DEL GAD MUNICIPAL DEL CANTÓN MEJÍA.

Proyecto de Titulación previo a la obtención del título de Ingeniería en Informática y Sistemas Computacionales.

AUTORAS:

Collaguazo Quinatoa María Belén

Toapanta Chilig Diana Nataly

TUTOR:

Ing. MSc. Alex Christian Llano

Latacunga – Ecuador

Febrero – 2020

UNIVERSIDAD TÉCNICA DE COTOPAXI

Ingeniería Informatica Y Sistemas Computacionales

DECLARACIÓN DE AUTORÍA

Nosotras, **COLLAGUAZO QUINATOA MARÍA BELÉN** y **TOAPANTA CHILIG DIANA NATALY,** declaro ser autoras del presente proyecto de investigación: **"IMPLEMENTACIÓN Y ADMINISTRACIÓN DE UN SERVIDOR DE DOMINIO, MEDIANTE SECURITY ACCOUNT MANAGER, PARA CENTRALIZAR LOS RECURSOS, SERVICIOS DE LAS TIC´S DEL GAD MUNICIPAL DEL CANTÓN MEJÍA"**, siendo el Ing. MSc. **Llano Casa Christian Alex** tutor del presente trabajo; y eximo expresamente a la Universidad Técnica de Cotopaxi y a sus representantes legales de posibles reclamos o acciones legales.

Además, certifico que las ideas, conceptos, procedimientos y resultados vertidos en el presente trabajo investigativo, son de mi exclusiva responsabilidad.

.....	.....
Collaguazo Quinatoa Maria Belén	Toapanta Chilig Diana Nataly
C.C: 050396047-8	C.C: 175146839-6

UNIVERSIDAD TÉCNICA DE COTOPAXI

Ingeniería Informatica Y Sistemas Computacionales

AVAL DEL TUTOR DE PROYECTO DE TITULACIÓN

En calidad de Tutor del Trabajo de Investigación sobre el título:
"IMPLEMENTACIÓN Y ADMINISTRACIÓN DE UN SERVIDOR DE DOMINIO, MEDIANTE SECURITY ACCOUNT MANAGER, PARA CENTRALIZAR LOS RECURSOS, SERVICIOS DE LAS TIC´S DEL GAD MUNICIPAL DEL CANTÓN MEJÍA", de **COLLAGUAZO QUINATOA MARIA BELÉN y TOAPANTA CHILIG DIANA NATALY**, de la carrera de INGENIERÍA EN INFORMÁTICA Y SISTEMAS COMPUTACIONALES, considero que dicho Informe Investigativo cumple con los requerimientos metodológicos y aportes científicos-técnicos suficientes para ser sometidos a la evaluación del Tribunal de Validación de Proyecto que el Consejo Directivo de la Facultad de CIENCIAS DE LA INGENIERÍA Y APLICADAS de la Universidad Técnica de Cotopaxi designe, para su correspondiente estudio y calificación.

Latacunga, Febrero, 2020

Ing. Llano Casa Alex Christian
CC: 050258986-4

TUTOR

UNIVERSIDAD TÉCNICA DE COTOPAXI

Ingeniería Informatica Y Sistemas Computacionales

APROBACIÓN DEL TRIBUNAL DE TITULACIÓN

En calidad de Tribunal de Lectores, aprueban el presente Informe de Investigación de acuerdo a las disposiciones reglamentarias emitidas por la Universidad Técnica de Cotopaxi, y por la Facultad de Ciencias de la Ingeniería y Aplicadas; por cuanto, las postulantes: **COLLAGUAZO QUINATOA MARIA BELÉN** y **TOAPANTA CHILIG DIANA NATALY** con el título de Proyecto de titulación: "**IMPLEMENTACIÓN Y ADMINISTRACIÓN DE UN SERVIDOR DE DOMINIO, MEDIANTE SECURITY ACCOUNT MANAGER, PARA CENTRALIZAR LOS RECURSOS, SERVICIOS DE LAS TIC´S DEL GAD MUNICIPAL DEL CANTÓN MEJÍA**" han considerado las recomendaciones emitidas oportunamente y reúne los méritos suficientes para ser sometido al acto de Sustentación de Proyecto.

Por lo antes expuesto, se autoriza realizar los empastados correspondientes, según la normativa institucional.

Latacunga, febrero del 2020

Para constancia firman:

Lector 1 (Presidente)
Ing. MSc. Villa Quishpe Manuel William
CC: 180338695-0

Lector 2
Ing. MSc. Rodriguez Barcenas Gustavo
CC: 175700135-7

Lector 3
Ing. MSc. Rubio Peñaherrera Jorge Bladimir
CC: 050222229-2

AGRADECIMIENTO

En primer lugar, agradezco a Dios por haberme permitido llegar hasta donde estoy, por llenarme de sabiduría en todo este tiempo recorrido, cuidarme desde el momento que empecé la carrera hasta el día de hoy.

Gracias a mi esposo y a mis suegros por haber estado conmigo en todo instante y acompañarme en los buenos y malos momentos vividos a lo largo de mi vida universitaria.

A mis padres y hermanos por su amor incondicional, gracias por creer en mí y nunca dejarme sola en este proceso universitario.

Un agradecimiento especial al Ing. Alex Llano por haber sido nuestro tutor de tesis y un amigo más en la Universidad, gracias por todos los conocimientos brindados en todo este tiempo.

Belén Collaguazo

AGRADECIMIENTO

Agradezco en primer lugar a Dios, por bendecirme con vida, amor, bondad y sobre todo mucha fortaleza, para culminar mi formación académica con éxito.

A mi Madre por brindarme mucha paciencia y apoyo durante todo este tiempo, hasta el presente. Por confiar en mí y nunca dejarme rendir por todos los obstáculos que surgieron en camino de este sueño, ya que sin ella no hubiese podido llegar hasta aquí.

A toda mi familia y amigos especialmente Jhenny y Ricardo, que nunca me han dejado rendirme y siempre motivándome para salir adelante, gracias por su bella amistad.

De la misma manera mis agradecimientos a la Universidad Técnica de Cotopaxi, a toda la Facultad de Ciencias de la Ingeniería y Aplicadas, por abrirnos las puertas a muchos estudiantes para cumplir con un sueño que muchos pensábamos que era algo imposible, a mis docentes por sabernos transmitir sus conocimientos, gracias a cada uno de ustedes por la dedicación y paciencia que nos han tenido durante esta etapa. De manera especial a mi tutor Ing. Alex Christian Llano Casa, quien nos ha guiado en este trabajo de tesis, demostrándonos su amistad, conocimientos, dedicación, esmero y paciencia.

Diana Toapanta

DEDICATORIA

Mi tesis va dedicado a mi Padre Celestial, quien fue mi guía, mi protector en el caminar de mi vida, bendiciéndome y dándome fuerzas para continuar con mis metas trazadas sin desfallecer, por cuidarme cada paso todos días hasta terminar con esta pequeña meta de mi vida.

A mi amado esposo Jhony Simba, se la dedico con todo mi amor por su sacrificio y esfuerzo en todo este tiempo que ha estado junto a mí, por darme una carrera para nuestro futuro y por creer en mi capacidad, aunque hemos pasado por momentos difíciles siempre ha estado brindándome su compresión cariño y amor.

A mi hija, mi amor grande Mikaela Simba por ser mi fuente de motivación para luchar cada día sin perder la fé y así poder emprender un camino mejor para nuestro futuro.

A mis amados padres y hermanos quienes que con sus palabras de aliento y motivación a la distancia me ayudaron a que continúe con mi meta, hasta lograrlo.

A mis queridos suegros por su gran amor y comprensión en este tiempo que me ayudaron con mi pequeña, para que siguiera delante y poder cumplir con mis ideales.

Belén Collaguazo

DEDICATORIA

El presente trabajo de investigación lo dedico principalmente a Dios y a mi abuelito que desde el cielo siempre me están llenando de bendiciones y por darme la fuerza para terminar una de mis metas más importantes.

A mi madre, la cual siempre me ha apoyado desde mis primeros pasos hasta la actualidad, demostrándome cariño, amor y enseñándome algo muy importante, en nunca rendirme y si tropiezo nunca decir no puedo y ser perseverante, hasta conseguirlo.

A mi hija la cual es el motivo fundamental para superarme mucho más, la cual, con toda su ternura, sus locuras y sus berrinches, me han motivado para no quedarme estancada y salir adelante, haciendo que mis días sean maravillosos con solo una palabra una expresión o un gesto que me brinda, y a mi novio Mauricio por siempre estar pendiente de mí y nunca dejarme sola en momentos difíciles.

A mis amigos Jhenny, Ricardo y Santiago, por haber llegado a mi vida, a llenarla de felicidad, por siempre estar apoyándome en todos mis sueños y locuras, gracias por su bella amistad.

Diana Toapanta

ÍNDICE GENERAL

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

UNIVERSIDAD TÉCNICA DE COTOPAXI

FACULTAD DE CIENCIAS DE LA INGENIERÍA Y APLICADAS

TÍTULO: "IMPLEMENTACIÓN Y ADMINISTRACIÓN DE UN SERVIDOR DE DOMINIO, MEDIANTE SECURITY ACCOUNT MANAGER, PARA CENTRALIZAR LOS RECURSOS, SERVICIOS DE LAS TIC´S DEL GAD MUNICIPAL DEL CANTÓN MEJÍA".

AUTORAS: Collaguazo Quinatoa María Belén

Toapanta Chilig Diana Nataly

RESUMEN

En el departamento de TIC´s del GAD Municipal del Cantón Mejía no existe un servidor de dominio, ya que trabajan de una forma tradicional, los usuarios están interconectados a una red, debido a esto los equipos no son administrables generando demora en el proceso de la creación de usuarios, unidades organizativas y equipos computacionales, por tal razón este proyecto de investigación propone dar una solución a la administración de recursos informáticos, mediante un Active Directory, permitiendo crear grupos para organizar, administrar y proteger los recursos de los equipos, con el fin de controlar y resguardar la información de los usuarios del GAD, se aplicó diferentes metodologías para la extracción y deducción de soluciones, realizando un análisis de las cualidades necesarias con las que debe contar el servidor de dominio y poner en práctica mediante un modelo experimental. Como resultado se obtuvo el control centralizado de los recursos informáticos, usuarios y equipos, evitando así diversos problemas en la red: como acceso no autorizado a los recursos por personas ajenas y pérdida de información laboral de la institución. Se concluye que con el servidor de dominio se puede gestionar las cuentas de los usuarios, grupo y equipos, dando de esta manera una organización de los recursos y servicios TIC´s en el GAD Municipal.

Palabras claves: Servidor de Dominio, centralizado, Active Directory, servicios, TIC´s.

TECHINICAL UNIVERSITY OF COTOPAXI

FACULTY OG ENGINEERING AND APPLIED SCIENCES

THEME: "IMPLEMENTATION AND ADMINISTRATION OF DOMAIN SERVER, BY A SECURITY ACCOUNT MANAGER, TO CENTRALIZE RESOURCES, SERVICES OF TIC´S OF THE DECENTRALIZED AUTONOMOUS GOVEMMENT OF MEJIA CANTON".

Author: Collaguazo Quinatoa Maria Belen

Toapanta Chilig Diana Nataly

ABSTRACT

At ICT Municipal GAD department of Mejia Canton there is no a domain server, since they work in a traditional way, users are interconnected to a network, because of this the equipment is not manageable generating delay in the process of the creation of users, units of organization and computer equipment, for this reason this research project proposes to provide a solution to the computer resources administration, through an Active Directory, allowing organize groups to manage and protect equipment resources, In order to control and safeguard the users information of the GAD, different methodologies were applied for the extraction and deduction of solutions, carrying out an analysis of the necessary qualities that the domain server must have and put into practice through an experimental model . As a result, centralized control of computer resources users and equipment was obtained, thus avoiding various problems on the network: such as unauthorized access to resources by outsiders and loss of labor information from the institution. It is concluded that with the domain server users accounts could be managed, group and teams, thus giving an organization of ICT resources and services to the Municipal GAD.

Keywords: Domain server, centralized, Active Directory, services, TIC´s.

UNIVERSIDAD TÉCNICA DE COTOPAXI

Centro Cultural de Idiomas

AVAL DE TRADUCCIÓN

En calidad de Docente del Centro de Idiomas de la Universidad Técnica de Cotopaxi; en forma legal **CERTIFICO** que: La traducción del resumen de la tesis al Idioma Inglés presentado por las señoritas Egresadas de la Carrera de Ingeniería en Informática y Sistemas Computacionales de la Facultad de Ciencias de la Ingeniería y Aplicadas: **Collaguazo Quinatoa María Belén y Toapanta Chilig Diana Nataly,** cuyo título versa **"Implementación y Administración de un servidor de dominio, mediante Security Account Manager, para centralizar los recursos, servicios de las TIC´s del GAD Municipal del Cantón Mejía",** lo realizaron bajo mi supervisión y cumple con una correcta estructura gramatical del idioma.

Es todo cuanto puedo certificar en honor a la verdad y autorizo a las peticionarias hacer uso del presente certificado de la manera ética que estimaren conveniente.

Latacunga, febrero del 2020

Atentamente,

.....

Lic. Marcelo Pacheco Pruna
DOCENTE CENTRO DE IDIOMAS
C.C. 050261735-0

CENTRO DE IDIOMAS

1. INFORMACIÓN GENERAL

Título del Proyecto

Implementación y administración de un servidor de dominio, mediante Security Account Manager, para centralizar los recursos, servicios de las TIC´s del GAD Municipal del Cantón Mejía.

Fecha de inicio:

Septiembre – 2019

Fecha de finalización:

Febrero – 2020

Lugar de ejecución:

Machachi – Cantón Mejía – Pichincha – Zona 2 – GAD Municipal del Cantón Mejía.

Facultad que auspicia:

Facultad de Ciencias de la Ingeniería y Aplicadas.

Carrera que auspicia:

Carrera de Ingeniería en Informática y Sistemas Computacionales.

Equipo de trabajo:

Tutor de Titulación

Ing. Alex Llano.

Coordinadoras del Proyecto

Collaguazo Quinatoa María Belén

Toapanta Chilig Diana Nataly

Área de Conocimiento:

Redes y Telecomunicaciones.

Línea de investigación:

Tecnologías de Información y Comunicación.

Sub líneas de investigación de la Carrera:

Diseño, implementación y configuración de redes y seguridad computacional, aplicando normas y estándares internacionales.

2. RESUMEN DEL PROYECTO

El presente proyecto de titulación propone dar una solución a la administración de recursos informáticos, desarrollando e implementando un servidor de Dominio mediante Security Account Manager en un entorno de Windows Server 2012, con el fin de obtener una estructura, que nos permita, crear grupos para administrar, organizar y proteger los recursos de los equipos, lo cual podemos controlar los niveles jerárquicos de los usuarios que están dentro del GAD Municipal del Cantón Mejía, resguardando la información, mediante la identidad basada en un protocolo de servicios de directorios cliente – servidor. De esto se encarga el controlador de dominio el cual crea un repositorio centralizado de contraseñas, esto para obtener una lista con nombres de usuarios y contraseñas así que estos estarán enlazados entre sí, lo que es más eficiente que tener en cada equipo diferentes contraseñas para cada recurso de la red. Una vez en el perfil de usuarios tendrán los servicios que el dominio asigna para el desarrollo de su actividad laboral, con esto nos enfocamos a el acceso a la información de forma controlada para salvaguardar la integridad de archivos, usuarios, grupos, dispositivos de red y periféricos. Para lo cual se aplicará metodologías y técnicas, para la extracción y deducción de soluciones para realizar un análisis de las cualidades necesarias con las que se debe contar el servidor de Dominio y ponerlas en práctica con un modelo experimental, un servidor de Dominio utilizando Security Account Manager, deberá contar con las condiciones necesarias para cumplir este objetivo, el fin es implementar un servidor con dichas características, una de las funciones principales a cumplir es los servicios integrados de autenticación y autorización a gran escala, más el comportamiento basado en las políticas de grupo para los usuarios del GAD Municipal del Cantón Mejía. Logrando con esto el control centralizado de los recursos, usuarios y equipos evitando así diversos problemas en la red: como, acceso no autorizado a los recursos del GAD por personas ajenas o ataques a los servidores que posee la institución, beneficiando no solo a los funcionarios sino a la comunidad en general, ofreciendo un ambiente confiable en el GAD Municipal de Mejía, que planteamos como principal objetivo de este proyecto.

3. JUSTIFICACIÓN DEL PROYECTO

La presente investigación surge por la necesidad de tener un servidor de dominio, que permita garantizar el acceso a recursos y servicios, del GAD Municipal del Cantón Mejía, tomando en cuenta que este tipo de servidor es de gran importancia dentro de una entidad, esto permite controlar una entidad administrativa con respecto al conjunto de equipos interconectados que existan dentro del municipio y las cuales pueden compartir información tales como usuarios, contraseñas, recursos entre otros.

Mediante la implementación del servidor de dominio, se pretende garantizar el acceso a recursos y servicios del GAD Municipal, para esto se procura al menos un equipo que sea el control principal del dominio, el cual proporciona servicio de autenticación y autorización centralizado. Esto puede implementarse bajo Windows como en Linux.

El servidor de dominio, está enfocado en brindar beneficios al GAD Municipal del Cantón Mejía, en el departamento de TIC´s, este proyecto tiene como impacto y relevancia la creación de un dominio basado en Windows Server 2012 R2, servicio dado por un sistema operativo muy bueno, que frece al municipio la capacidad de administrar los recursos de una manera segura, dando como resultado el aprovechamiento total por parte del departamento de TIC´s y a su vez a los usuarios del municipio.

4. BENEFICIARIOS DEL PROYECTO

Beneficiarios Directos

- Administrador del área de redes y Telecomunicaciones.

Beneficiarios Indirectos

- Departamento de TIC´s y el personal administrativo que pertenecen al GAD Municipal del Cantón Mejía.

5. EL PROBLEMA DE INVESTIGACIÓN

Un tema de gran preocupación para el hombre es de asegurar la información, en la antigüedad, grandes cantidades de información eran almacenadas en bodegas inmensamente grandes bajo llave, y aun así, que alguien pueda robar esa información podía resultar una tarea muy complicada; con los avances de la información esto ha ido cambiando cada vez más al momento de almacenar los datos, con la tecnología del microchip se puede almacenar grandes cantidades de información en dispositivos cada vez más pequeños, esto ha brindado mucha facilidad a la

hora de transportarlos, pero también ha resultado más difícil mantenerlos seguros. La interconexión de redes de trabajo que existen en la actualidad, si bien han brindado facilidad de acceso a los mismos, representa también un riesgo. Por esta razón muchas empresas desarrolladoras de software y entidades públicas alrededor de Latinoamérica han creado herramientas para controlar el acceso a los datos, herramientas como el Active Directory, del sistema operativo Windows Server 2008 R2 Enterprise o Windows Server 2012, esta herramienta brinda una amplia gama de opciones para gestionar el acceso al sistema. Windows también posee algunas herramientas para la encriptación de datos, como es BitLocker que se encuentra en las versiones Enterprise y Ultimate de Windows 7. (Jimenéz & Orellana, 2012)

A nivel superior en el Ecuador las instituciones educativas y a nivel mundial, han experimentado los grandes cambios tecnológicos que ha sufrido el planeta, por ende, contar con una estructura de red basada en las nuevas tecnologías que permita ofrecer a las entidades investigadoras, la posibilidad de enlazar conocimiento con el mundo, es de vital importancia, y de esta manera optimizar sus niveles académicos. (Ocampo & Vivanco, 2015)

En la provincia de Pichincha del Cantón Mejía en la Parroquia de Machachi, se observa que, en el GAD Municipal, en el departamento de TIC´s, su labor principal es ser el encargado de todos los sistemas informáticos que existe en la entidad y proteger los aspectos fundamentales de la información tales como la integridad, confidencialidad y disponibilidad. Con lo cual hemos observado que el GAD Municipal no cuenta con un servidor de dominio, ya que trabajan de una forma tradicional porque los usuarios están integrados en grupos de trabajo interconectados en una red, esto ha causado que los equipos no sean administrables y demora en el proceso de crear usuarios en el ordenador al momento que ingresan personal nuevo. Con este proyecto de investigación se espera establecer bases para que, si la red se extiende en el GAD o existen cambios de personal, el proceso sea lo más sencillo posible, mediante una infraestructura que nos permite más equipos a la red sin incrementar la complejidad.

6. OBJETIVOS:

6.1. Objetivo General

Implementar una solución a la administración de recursos TIC´s con Security Account Manager, mediante un controlador de dominio usando un protocolo de servicios de directorios cliente/servidor en el GAD Municipal del Cantón Mejía.

6.2. Objetivos Específicos

- Analizar la información teórica relacionada con Security Account Manager, directorio activo y protocolos.
- Realizar una investigación de campo en el GAD Municipal de Mejía, para recopilar información sobre la infraestructura actual de los equipos y la conexión con los servidores.
- Implementar un servidor de dominio funcional, seguro y confiable para garantizar la creación de los recursos centralizados y la unión de equipos sobre la red del GAD Municipal del Cantón Mejía.
- Administrar la autenticación y autorización a gran escala de los usuarios en el acceso a recursos u otros equipos del GAD Municipal del Cantón Mejía.

7. ACTIVIDADES Y SISTEMA DE TAREAS EN RELACIÓN A LOS OBJETIVOS PLANTEADOS.

Tabla 1. Sistema de tareas en relación a los objetivos planteados.

OBJETIVOS	ACTIVIDADES (TAREAS)	RESULTADO DE LA ACTIVIDAD	MEDIOS DE VERIFICACIÓN
Analizar la información teórica relacionada con Security Account Manager, directorio activo y protocolos.	**Tarea 1:** Búsqueda de información en las bases de datos científicas. **Tarea 2:** Investigar las bases teóricas del proyecto. **Tarea 3:** Análisis de los contenidos de los documentos identificados.	La adquisición de información oportuna acerca del tema de investigación. La investigación de estudios potenciales.	• Búsqueda de información en las bases de datos científicas, Scholar, Scielo, RedaLyc, entre otros.
Realizar una investigación de campo en el GAD Municipal de Mejía, para recopilar información sobre la infraestructura actual de los equipos y la conexión con los servidores.	**Tarea 1:** Realizar una entrevista al director de TIC´s. **Tarea 2:** Conocer que tan seguro es la red del GAD. **Tarea 3:** Observar la información recopilada para su previo análisis.		

Implementar un servidor de dominio funcional, seguro y confiable para garantizar la creación de los recursos centralizados y la unión de equipos sobre la red del GAD Municipal del Cantón Mejía.	**Tarea 1:** Implementar el servidor de dominio, obtenido del proyecto de investigación.	Proyecto de Investigación.	• Investigación documental. • Servidor Security Account Manager.
Administrar la autenticación y autorización a gran escala de los usuarios en el acceso a recursos u otros equipos del GAD Municipal del Cantón Mejía.	**Tarea 1:** Realizar un diagnóstico previo para conocer si existen riesgos, vulnerabilidad y amenazas dentro de la institución. **Tarea 2:** Observar la inseguridad que se puede presentar en las diferentes áreas informáticas de la institución. **Tarea 3:** Administrar los accesos de usuarios, grupos y equipos computacionales.	Proyecto de investigación. Administración de accesos y garantía de los recursos.	• Investigación de campo. • Investigación documental.

Fuente: Grupo investigador.

8. FUNDAMENTACIÓN CIENTÍFICA TÉCNICA

8.1. Antecedentes

8.1.1. Sistema Operativo Windows Server 2008

Windows Server 2008, es el nombre del sistema operativo para servidores de Microsoft. Es el sucesor de Windows Server 2003 distribuido al público casi cinco años antes. Con Windows Server 2008 se puede desarrollar, entregar y administrar experiencias de usuarios y aplicaciones, proporcionando una alta seguridad de infraestructura de red, y aumentar la eficiencia tecnológica y el valor dentro de su organización. (Lopez, 2013)

Es un sistema operativo para servidores diseñada para Microsoft con características de virtualización, administración y seguridad, estos sistemas operativos son los más conocidos para las personas y los más fáciles de utilizar. (Lopez, 2013)

Figura 1. Sistema Operativo Windows Server 2008.

Fuente: (Lopez, 2013)

8.1.1.1. Características de Windows Server 2008

Hay algunas diferencias con respecto a la arquitectura del nuevo Windows Server 2008, que pueden cambiar drásticamente la manera en que se usa este sistema operativo. Estos cambios afectan a la manera en que se gestiona el sistema hasta el punto de que se puede llegar a controlar el hardware de forma más efectiva, se puede controlar mucho mejor de forma remota y cambiar radical la política de seguridad. Entre las mejores que se incluyen están: (Cruz, Pacheco, & Vanegas, 2014)

- Nuevo proceso de reparación de sistemas NTFS: Proceso en segundo plano para reparar los archivos dañados.

- Creación de sesiones de usuario en paralelo: reduce tiempos de espera en el terminal Services y en la creación de sesiones de usuario a gran escala.
- Cierre limpio de Servicios.
- Sistema de archivos SMB2: de 30 a 40 veces más rápido el acceso a los servidores multimedia.
- AddressSpace Load Randomization (ASLR): Protección contra malware en la carga de controladores en memoria.
- Virtualización de Windows Server: mejoras en el rendimiento de la virtualización
- PowerShell: inclusión de una consola mejorada con soporte GUI para administración.

8.1.1.2. Funciones de Windows Server 2008

Windows Server 2008 es un sistema operativo que está compuesta por varias funciones y características lo que hace diferente su arquitectura de configuración respecto a los demás procesadores. En la siguiente tabla se detalla las funciones que tiene Windows Server 2008.

Tabla 2. Principales funciones de Windows Server 2008.

FUNCIONES	DEFINICIÓN
Características de .NET Framework 3.0	Esto nos proporciona las API del framework 3.o, para el desarrollo de las aplicaciones.
Cifrado de unidad BitLocker	Proporciona características de seguridad basadas en hardware para la protección de datos sentibles mediante cifrado de volúmenes completos.
Extensiones de servidor BITS.	Permite la relación de transferencias inteligentes en segundo plano.
Kit de administración de connection manager.	Proporciona la funcionalidad necesaria para la creación de perfiles Connection Manager
Experiencias de uso	Proporciona las funciones adicionales de escritorio de Windows Vista como: reproductor de Windows Media,
Administración de directivas de grupo	Herramienta para la administración centralizada para las directivas de grupo.
Clúster de conmutación por error	Proporciona alta disponibilidad a los servicios y aplicaciones.

Fuente: Grupo investigador.

8.1.1.3. Ediciones de Windows Server 2008

A continuación, se describen las diferentes ediciones que posee Windows Server 2008.

Tabla 3. Ediciones de Windows Server 2008.

EDICIONES	DESCRIPCIÓN
Windows Server 2008 Standard Edition	Es un complemento del sistema operativo de red para servidores que puede utilizarse en organizaciones de tamaño pequeño y moderado.
Windows Server 2008 Enterprise Edition	Es un complemento del sistema operativo de red para servidores, orientado a organizaciones más grandes, sobre todo la relaciona con el comercio electrónico.
Windows Server 2008 Datacenter Edition	Se relaciona con el almacenamiento de datos y procesamiento de transacciones en línea. Brinda todas las capacidades de Enterprise Edition.
Windows Web Server 2008.	Es un sistema operativo de servidor, limitado al alojamiento de sitios Web y servicios de aplicaciones web.
Windows Server 2008 para sistemas Itanium.	Este sistema operativo está limitado para procesadores de 64 bits Itanium 2 de Intel. Tiene disponible las funciones del servidor Web y la entrega de aplicaciones.

Fuente: (Matthews, 2013)

8.1.2. Sistema Operativo Windows Server 2012

Windows Server 2012 R2 provee a un administrador una plataforma completa, a nivel de administración de dominio AD, virtualización o implantación de un sistema de cloud computing. El sistema operativo nos ofrece una plataforma de virtualización que permite la creación de un entorno totalmente aislado. El entorno se adapta, además, a las necesidades con el objetivo de garantizar fiabilidad y un rendimiento óptimo de los recursos. (Bonnet, 2014)

Windows Server 2012 nos ofrece una plataforma segura y confiable para poder albergar las aplicaciones y los servicios web, es de fácil utilización y posee nuevas funciones útiles con mayor protección y control, estas son las características fundamentales de este sistema operativo.

8.1.2.1. Ediciones de Windows Server 2012

En la tabla 4 vamos a ver cuáles son las principales ediciones que tienes Windows Server 2012.

Tabla 4. Principales ediciones de Windows Server 2012.

EDICIÓN	DESCRIPCIÓN
Windows Server 2012 R2 Datacenter	Es utilizado para un entorno altamente virtualizado que requiere características de alta disponibilidad, incluida a la agrupación en clústeres.
Windows Server 2012 R2 Standard	Para un entorno no virtualizado o poco virtualizado en el que se desee incluir características de alta disponibilidad, incluida la agrupación en clústeres.
Windows Server 2012 R2 Essentials	Para pequeñas empresas con hasta 25 usuarios, especialmente aquellas empresas que quieran implementar su primer servidor.
Windows Server 2012 R2 Foundation	Para pequeñas empresas con hasta 15 usuarios (solo disponible a través de partners OEM directos).

Fuente: Grupo investigador.

8.1.2.2. Principales características de Windows Server 2012.

a. Virtualización de servidor

La virtualización permite tener un ahorro mayor y maximizar las inversiones en hardware de servidor mediante la consolidación de los servidores como máquinas virtuales en un único host físico. (Microsoft A. , 2015)

b. Almacenamiento

Sin importar a plataforma de almacenamiento que se esté utilizando. Windows Server 2012 R2 puede optimizar el almacenamiento: por ejemplo, en redes SAN. (Microsoft A. , 2015)

c. Redes

Una buena gestión de red es primordial para que todo el sistema funcione de una forma correcta y se pueda brindar los servicios requeridos por los usuarios para cuando estos lo necesiten. También se puede administrar una red completa con un único servidor. (Microsoft A. , 2015)

d. Automatización y administración de servidores

A partir de un enfoque de administración basado en estándares, Windows Management Framework brinda una plataforma común para la automatización e integración con el fin de

ayudar a automatizas las tareas rutinarias con herramientas como Windows PowerShell. (Microsoft A. , 2015)

e. Plataforma de aplicaciones y web

Windows Server 2012 R2 se basa en la tradición de la familia Windows Server como plataforma de aplicaciones demostrada, con miles de aplicaciones compiladas e implementadas y una comunidad de millones de desarrolladores expertos y cualificados perfectamente instaurada. (Microsoft A. , 2015)

f. Protección de la información

Las soluciones de protección de la información que ofrece Microsoft permiten administrar una única identidad para cada usuario, en aplicaciones tanto locales como basadas en la nube. (Microsoft A. , 2015)

8.1.3. Sistema Operativo Windows Server 2016

Windows Server 2016 es el sistema operativo preparado para la nube que ofrece nuevas capaz de seguridad e innovaciones inspiradas en Azure para las aplicaciones y la infraestructura que impulsan su empresa. Aumenta la seguridad y reduce los riesgos empresariales con varias capas de protección integradas en el sistema operativo. Haga evolucionar su centro de datos con el objetivo de ahorrar dinero y ganar flexibilidad gracias a tecnologías de centro de datos definido por software inspiradas en Microsoft Azure. Innove con mayor rapidez gracias a una plataforma de aplicaciones optimizada para las aplicaciones que ejecuta en la actualidad, así como para las aplicaciones nativas de la nube de mañana. (Microsoft, 2016)

8.1.3.1. Novedades de Windows Server 2016

a. Host de protección de los recursos. – Esta funcionalidad permite evitar el uso excesivo de los recursos por parte de una máquina virtual, con el objetivo de evitar una degradación de rendimiento de la máquina host. (Bonnet, 2018)

b. Nested Virtualization (virtualización anidad). – Esta funcionalidad permite agregar el rol Hyper-V en una máquina virtual Hyper-V que ejecuta Windows Server 2016. También nos permite albergar máquinas virtuales. (Bonnet, 2018)

c. Actualizaciones del clúster Hyper-V. – Se ha facilitado la actualización de un clúster con Windows Server 2012 R2. Ahora es posible agregar un nodo Hyper-V en un clúster Hyper-V Windows Server 2012 R2. (Bonnet, 2018)

d. Almacenamiento QoS. – Ahora es posible la creación de reglas QoS en un SOFS (Scale-Out File Server). Estas podrán aplicarse a los discos duros virtuales de las máquinas. Esta funcionalidad permite llevar a cabo una mejor gestión de almacenamiento en términos de carga. (Bonnet, 2018)

8.1.3.2. Ediciones de Windows Server 2016

Las ediciones de Windows Server 2016 se han racionalizado con el objetivo de respaldar mejor los cambiantes requisitos empresariales de hoy día.

A continuación, vamos a detallar cada una de las ediciones que tiene Windows Server 2016 y cuál es su respectiva descripción.

Tabla 5. Ediciones de Windows Server 2016

EDICIONES	DESCRIPCIÓN
Windows Server 2016 Datacenter	Se trata de la versión más completa destinada a los sistemas de información fuertemente virtualizados y a los entornos en Cloud. Permite alojar un número ilimitado de máquinas virtuales.
Windows Server 2016 Standard	Es útil en los entornos con servidores físicos que utilicen poco o nada la virtualización.
Windows Server 2016	Está edición remplaza a Small Business Server Essentials. Está limitada a una única instancia física o virtual, con un máximo de 25 usuarios y 50 periféricos.
Windows Hyper-V Server	Se trata de una versión Core, que incluye todas las funcionalidades relacionadas con la virtualización, porque está destinada a albergar máquinas virtuales.
Windows Storage Server 2016 o Standard Edition	Está dedicada a la gestión de almacenamiento dentro de su red. Está versión permite conectar 50 usuarios.

Fuente: (Vanjones, Deman, Elmaleh, & Ddesfarges, 2018)

8.1.4. Comparación de los Sistemas Operativos Windows Server 2008, 2012 y 2016

En la tabla 6, se va hacer una comparación de los sistemas operativos Server ya que con las ventajas que pondremos se podrá llegar a la conclusión de cual Windows Serve este más acto para la implementación del Servidor de Dominio.

Tabla 6. Cuadro Comparativo de los Sistemas Operativos Windows Server.

SISTEMAS OPERATIVOS	WINDOWS SERVER 2008	WINDOWS SERVER 2012	WINDOWS SERVER 2016
Descripción	En una base tecnológica rentable y de un nivel básico orientada a propietarios de pequeñas empresas y generalistas en TI que brindan soporte a pequeñas compañías.	Windows Server 2012 es un sistema que permite compartir archivo e impresoras, acceder remotamente al servidor y proporciona seguridad en los recursos.	Es un sistema operativo que posee robustez y estabilidad en la cual este realiza actualizaciones en un núcleo manteniendo los servicios instalados de manera segura y con nuevas funciones.
Ventajas	- Posee robustez con capacidades de virtualización avanzadas. - Diseñado para incrementar la confiabilidad y la flexibilidad de la infraestructura de red con el objetivo de disminuir tiempo y costo de implementación.	- Proporciona una base de red para la configuración y administración de equipos de manera centralizada. - Proporciona una interfaz de Windows de usuarios para el manejo de sistema.	- Espacio de almacenamiento directo. - Contenedores de Windows Server. - Servidor de archivo en escala horizontal. - Resistencia de almacenamiento de máquinas virtuales.

Fuente: (Armijos & Candelario, 2018)

8.1.5. CentOS

CentOS (Community Enterprise Operating System) Linux proporciona una plataforma informática, es decir, un sistema operativo (SO), de código libre y abierto a cualquier persona que desee utilizarlo. Es una distribución mantenida por la comunidad y derivada de los paquetes fuentes liberados al public por red Hat para "Red Hat Enterprise Linux" (RHEL). De esa manera, CentOS Linux está enfocado en ser operacionalmente compatible con RHEL. El proyecto CentOS, principalmente, cambia paquetes para eliminar las marcas comerciales y trabajos artísticos de red Hat. (García, Garrido, Gómez, & Romero, 2015)

8.1.5.1. CentOS 7

La redistribución de CentOS Linux es totalmente libre y no hay que pagar para poder usarlo, además desde la versión de CentOS 5 cada versión de CentOS es mantenida por 10 años, por medios de actualizaciones de seguridad, la duración de los intervalos de mantenimiento ha variado a lo largo del tiempo con relación a los paquetes fuentes liberados. Una versión nueva de CentOS es liberada aproximadamente cada 2 años y cada versión de CentOS es periódicamente actualizada, normalmente cada 6 meses para mantenimiento, confiable, predecible, reproducible y fácil de instalar y utilizar. Por poner un ejemplo, la última versión 7, recibirá actualizaciones de seguridad hasta el 30 de junio de 2024. (García, Garrido, Gómez, & Romero, 2015)

8.2. Marco Referencial

Con el propósito de obtener información acerca de un servidor de dominio, se ha buscado fuentes bibliográficas de proyectos de varias universidades (no se pudo encontrar ningún proyecto igual al tema de investigación), encontrando únicamente proyectos similares al tema.

Universidad Nacional Autónoma de México, Facultad de Ingeniería, los estudiantes Yosimar Olvera Oliva y Julio Cesar Rizo Gaona; con el tema **"Implementación de un dominio en el centro de apoyo a la docencia del Cele para la optimización de sus recursos y servicios"** (Yosimar Olvera & Rizo Gaona, 2013)**,** expresan las siguientes conclusiones:

Con la implementación de este dominio se logró centralizar la administración de los principales recursos del centro, es decir, los usuarios y la información. Además, se centralizo también la gestión del software utilizando en el centro y de las actividades de configuración de los equipos, desde la instalación de sistemas operativos y programas, hasta configuraciones importantes de seguridad.

Además de los beneficios obtenidos sobre la administración de los recursos y de la información, el implementar el dominio. Significo también mejoras importantes para la seguridad en el centro, ya que estos tópicos, administración y seguridad, están intrínsecamente relacionados, dado que una correcta administración conlleva a tener el escenario ideal para la implementación o preservación de los servicios de seguridad.

Otro punto que se logró completar de todo fue la estrategia que se planteó para mantener siempre en funcionamiento el controlador de dominio para brindar los principales servicios.

El estudiante Luis Alberto Mungabusi Sisa con el tema: **"Implementación de una distribución GNU/LINUX LSBS para la autenticación de los usuarios y la seguridad de los recursos de red de la Cooperativa de Ahorro y Crédito Esencia Indígena Ltda"** (Mungabusi, 2016)**,** expresa lo siguiente:

Luego del análisis de las distribuciones GNU/Linux Small Business Server, se pudo observar que la distribución Zentyal versión 4.0 es la más que cubre los requerimientos de la Cooperativa.

Se podría decir que la presente solución reduciría el costo de licenciamiento de software consecuentemente existe un costo adicional del hardware que se utilice, la confirmación y soporta de la misma.

La propuesta planteada facilita a los administradores de red gestionar adecuadamente las políticas de seguridad conjuntamente con los usuarios, ya que los servidores de las agencias se sincronizan con el servidor principal de manera inmediata, permitiendo así realizar los cambios en diferentes servidores.

En la Universidad Técnica de Cotopaxi, Facultad de Ciencias de la Ingeniería y Aplicadas, con el tema: **"Migración de Infraestructura de Servicios Microsoft (Active Directory, Exchange) de Windows server 2008 R2, hacia Windows server 2012 R2, utilizando la metodología MSF (Microsoft Solucions Framework), para mejorar los servicios tecnológicos de la empresa COBISCORP S.A",** (Gualotuña, 2016)**,** expresa las siguientes conclusiones.

El análisis de la información recolectada permitió comprender de mejor manera los conceptos necesarios para la implementación del presente proyecto.

A través de la información recolectada en la empresa se logró conocer el estado y la situación actual de los servicios que brinda la empresa.

Se aprovecho convenientemente la metodología Microsoft Solutions Framework para la ejecución del proyecto, cumpliendo con los puntos específicos en cada fase de la metodología, lo que ayudo en el desarrollo exitoso de la migración.

Las características de las nuevas máquinas virtuales con Windows server 2012 Standard R2, cumplieron con los requerimientos iniciales del proyecto, logrando que los servicios se mantengan estables y en funcionamiento.

En la Universidad Nacional de México, facultad de Ingeniería, el estudiante Aguilar Marco Antonio, con el tema **"Dominio para la Administración centralizada de recursos de cómputo",** (Aguilar, 2013)**,** reitera lo siguiente:

Con la base en el objetivo de este trabajo el cual consistía en la disminución de la carga de trabajo y mantenimiento de los equipos para los encargados del laboratorio de redes y seguridad de la facultad de ingeniería, por medio de una administración centralizada se puede constatar que fue alcanzado satisfactoriamente.

A lo largo de la implementación y la fase de pruebas en producción se detectaron algunos errores no previstos mismos que fueron corregidos lo más pronto que fue posible. Esta situación nos brindó la posibilidad de ver otras necesidades del laboratorio que no se tenían contempladas.

Otro aspecto que cabe resaltar, es que se ayudó a garantizar un mejor y correcto uso de los equipos de cómputo optimizado de manera que se pueda compartir recursos y así como la restricción de acceso a sitios como lo son redes sociales, con esto se logró un uso más adecuado de los equipos para actividades meramente académicas durante las clases prácticas.

8.3. Aspectos Teóricos

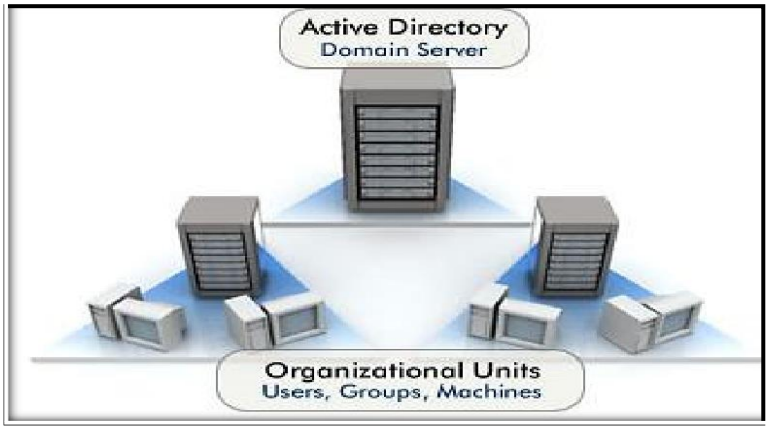
8.3.1. Servicio de directorio

Un directorio es como una base de datos, pero en general contiene información más descriptiva y basada en atributos. La conclusión que se extrae de esta situación, es que el servicio de directorio es un conjunto complejo de componentes que pueden trabajar de una forma cooperativa para prestar un servicio. (Calzada, 2014)

Es importante, el servicio de directorio porque nos proporciona una manera consistente de nombrar, describir, administrar y asegurar información acerca de dichas entidades u objetos,

actuando como una capa de abstracción entre los usuarios y los recursos, en la Figura 2. Se muestra los componentes de la estructura lógica de un directorio activo. (Calzada, 2014)

Figura 2. Estructura lógica del directorio activo.



Fuente: (Calzada, 2014)

8.3.1.1. Protocolos de Acceso

El protocolo que en sus inicios otorgaba el acceso a un directorio activo era el protocolo de Acceso a directorios DAP, el cual delimitaba los servicios para controlar las comunicaciones usuario-directorio y viceversa, para que el cliente tenga acceso completo a la información del directorio.

DAP e un protocolo que resulto ser extremadamente pesado, operaba sobre el modelo OSI y requería una cantidad significativa de recursos computacionales; por lo que LDAP nació como respuesta para simplificar el acceso al directorio X.500. (Romero, 2018)

Por otro lado, el protocolo ligero de acceso a directorios LDAP, opera sobre el modelo de referencia TCP/IP, compartiendo la misma función con su antecesor DAP, cuya ventaja radica en el uso de una menor cantidad de recursos, haciéndolo más viable a la hora de poner en producción un directorio.

8.3.2. LDAP (Protocolo Ligero de Acceso a Directorios)

LDAP (Protocolo Ligero de Acceso a Directorios) es 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 es considerado una base de datos (aunque su sistema de almacenamiento puede ser diferente) a la que pueden realizarse consultas. (Oleas, 2013)

El beneficio de configurar LDAP es manejar la información, en este caso de los usuarios de una manera, jerárquica y organizada para poder efectuar la autenticación de los usuarios que requieran el uso de una computadora dentro de un laboratorio. La información de los datos de autenticación se validará de una forma segura para los usuarios brindando a cualquier institución, empresa pública o privada la facilidad de poder gestionar la información, optimizar recursos y llevar un control automatizado de dicha información. (Oleas, 2013)

LDAP está basado en el protocolo X.500 para compartir directorios, y contiene esta información de forma jerarquizada y mediante categorías para proporcionarnos una estructura intuitiva desde el punto de vista de la gestión por parte de los administradores. (Castillo, 2019)

8.3.2.1. Funciones de LDAP

Vamos a enumerar algunas funciones que podemos aplicar con LDAP.

- Empleo como sustituto para el servicio NIS.
- Autenticación de usuarios de aplicaciones web.
- Autenticación de usuarios de sistemas operativos.
- Autenticación de usuarios con NFS en rede Unix.
- Autenticación de usuarios con Samba en redes heterogéneas.
- Encaminamiento de correo (postfic, sendmail).
- Libretas de direcciones para clientes de correo como: Mozilla, Evolution.

8.3.2.2. Características del LDAP

- Está basado en el modelo cliente - servidor.
- Organiza la información de modo jerárquico, utilizando directorios.
- Es capaz de programar sus directorios a otros servidores LDAP.
- Tiene un API de programación definido.

8.3.2.3. Funcionamiento de LDAP

El funcionamiento del acceso y administración es muy similar a Active Directory de Windows. Cuando el cliente LDAP se conecta con el servidor, podrá realizar dos acciones básicas, bien consultar y obtener información del directorio, o modificarla. (Castillo, 2019)

8.3.3. Active Directory

Active Directory es el núcleo principal de la infraestructura de TI de cada empresa en el mundo y la primera capa para crear seguridad, cumplimiento y automatización de usuarios y computadoras. (Iperius, 2019)

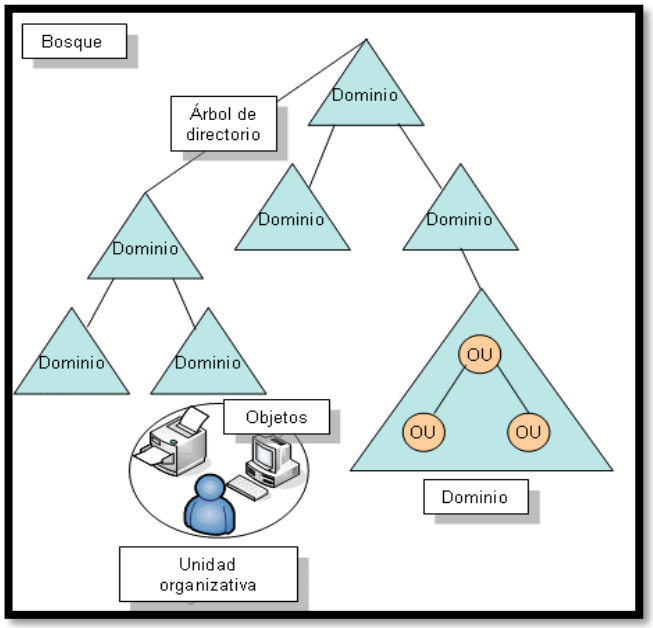
Una característica importante del Active Directory es la posibilidad de extender el esquema para agregar nuevas columnas, propiedades y valores. Algunas aplicaciones, como Exchange Server, usan Active Directory para agregar sus componentes y características para leer propiedades y evita usar sistemas. (Iperius, 2019)

8.3.3.1. Estructura Lógica

Active Directory tiene como características globales, brindar seguridad ante el almacenamiento de la información de sus clientes, los mismos que se representan entidades u objetos dentro de la estructura lógica, en la Figura 4, se muestran los componentes de dicha estructura.

La estructura lógica nos brinda una buena administración de los recursos de la red organizativa, permitiendo que el Active Directory nos pueda proporcionar un almacenamiento seguro de la información.

Figura 3. Estructura Lógica del Active Directory.



Fuente: (Ruiz P. , 2013)

A continuación, vamos a enumerar los componentes que tiene la estructura lógica del Active Directory.

a) Dominio

Un dominio es una colección de objetos dentro del directorio activo en la cual forman parte de un subconjunto administrativo. Actualmente existen diferentes dominios dentro de un bosque, cada uno de ellos contiene una propia colección de objetos y unidades organizativas. Para la implementación de un dominio en el directorio activo se utiliza el protocolo DNS en la cual se requiere al menos de un servidor instalado en la red. (Ruiz P. , 2013)

b) Objetivo

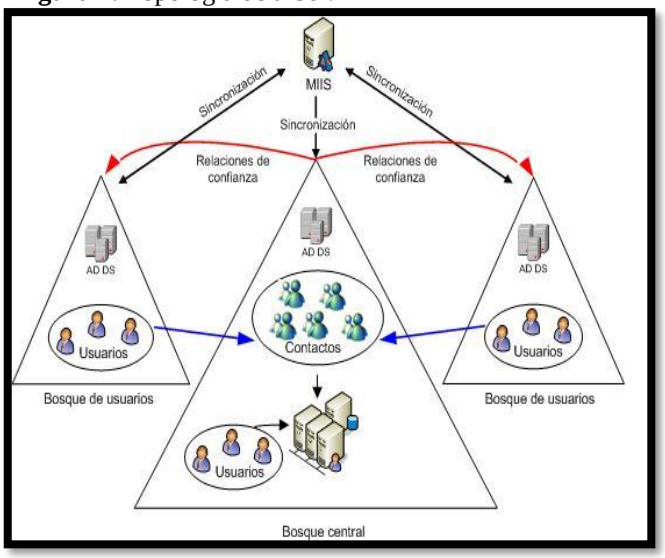
Son nombres que representan un recurso de la red. Los atributos de cada recurso son las características de cada objeto. (Gordillo, 2014)

Son objetos son componentes básicos de la estructura lógica. Algunos objetos nos permiten representar entidades individuales de la red, los cuales pueden ser un usuario y un equipo, los objetos están denominados como hojas que no pueden contener otros objetos.

c) Árboles

Un árbol es una colección de dominios que dependen de una raíz común y se encuentran organizados como una estructura jerárquica, dicha jerarquía también es representada por un espacio de nombres de dominio común. El objetivo de crear una infraestructura del árbol de dominio es la de fragmentar la información del directorio activo replicándolo solo las partes necesarias para disminuir el consumo de ancho de banda en la red. (Ruiz P. , 2013)

Figura 4. Topología de árbol.



Fuente: (Microsoft, 2017)

d) Unidades organizativas

Es un contenedor de objetos que se los organiza con el fin de poder administrarlos de una mejor manera, a estos se les puede delegar políticas de dominio, podemos para aplicar distintas configuraciones sobre los tipos de objetos que tengamos dentro. (Gordillo, 2014)

Las unidades organizativas nos ayudan a la estructuración de los objetos como usuarios y equipos, ya que con un adecuado orden se facilita la localización y administración de usuarios y grupos, además de eso las unidades organizativas pueden estar anidadas en otras unidades organizativas, lo que nos permite la administración de los objetos con más facilidad.

e) Bosques

El bosque es un conjunto de uno o más dominios que comparten una misma estructura lógica, catálogo global, esquema y configuración. Una vez se genera el primer controlador de dominio, se debe establecer el nombre del bosque el cual corresponde también el primer nombre del Dominio, un ejemplo sbeltran.com. Cada uno de los bosques es independiente y no puede tener comunicación con otro bosque a no ser que tenga el método para establecer conexiones entre diferentes compañías o en caso de que haya una combinación entre diferentes estructuras. Cuando se establece el nombre del bosque, este no se debe cambiar y debe ser exclusivo, una excepción es que exista un modelo simple y no se hubiesen realizado cambios por otro software. (Beltrán, 2019)

8.3.3.2. Estructura Física

Se usa para configurar y administrar el tráfico de red. Entender los componentes de la estructura física del DA es importante para optimizar el tráfico de red y el proceso de logon. Se compone de:

- Sitios

Determina la forma que debe replicarse la información de directorio y como debe tratarse las solicitudes de servicio de equipos los que son asignados a sitios, estos son una combinación de una o más subredes IP (Internet Protocol) conectadas en enlaces de alta velocidad, las cuales constituyen una forma sencilla y eficaz para representar agrupamiento en la red. (Hernández, Martínes, & Martín, 2016)

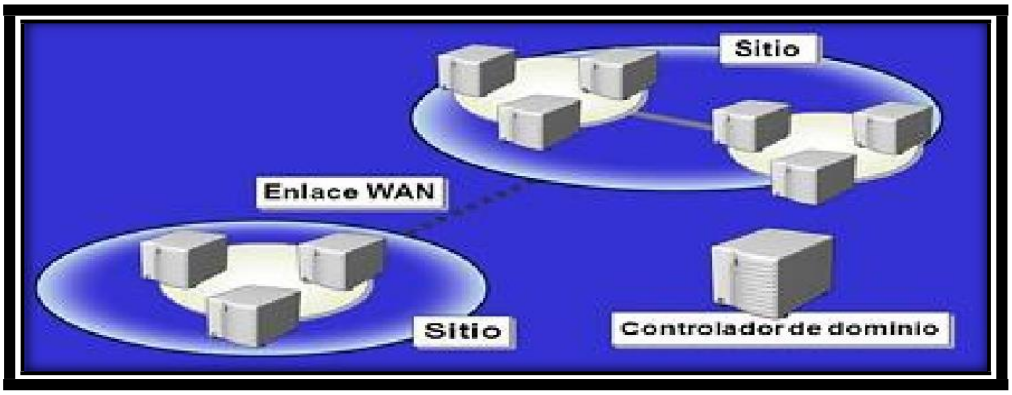
Los sitios son considerados como grupos de equipos conectados correctamente. Al momento de establecer un sitio, los controladores de dominio de un único sitio se comunican con frecuencia.

- Controlador de dominio

Es donde se almacena una copia de directorio, que almacenan datos y administran las interacciones entre el usuario y el dominio, como los procesos de inicio de sesión, la autenticación y las búsquedas de directorio. También administra los cambios de directorio y los replica a otros controladores de dominio del mismo dominio. (Hernández, Martínes, & Martín, 2016)

Es un dominio donde se puede identificar varios controladores del mismo asociado de modo que cada uno de ellos representa un rol diferente del directorio activo.

Figura 5. Estructura física del Active Directory.



Fuente: (Ortiz, 2015)

8.3.3.3. Ventajas que puede proporcionar el Active Directory dentro de una organización:

- La seguridad de la información: El control de acceso se puede definir no solo para cada objeto del directorio, sino también hará cada una de las propiedades del objeto.
- La administración basada en políticas: Establece un conjunto de normas de la empresa.
- La capacidad de ampliación: Los administradores tienen la posibilidad de agregar nuevos objetos de esquema y nuevos atributos.
- Integración con DNS (Domain Name System): Utiliza el Sistema de nombres de dominio, que es un servicio estándar de internet que traduce de equipos host a direcciones IP numéricos.

- Las consultas Flexibles: Los usuarios y administradores pueden utilizar el comando buscar para encontrar rápidamente un objeto en la red por sus propiedades. (Hernández, Martínes, & Martín, 2016)

8.3.4. Security Account Manager

Administrador de cuentas de seguridad (SAM). – Es una base de datos que se encuentra en equipos que ejecutan sistemas operativos Windows y que almacenan las cuentas de usuario y los descriptores de seguridad de los usuarios en el equipo local. (Microsoft, 2017)

Las contraseñas de los usuarios se almacenan en formato hash.

8.3.5. Cuentas de usuarios

Active Directory contiene muchos tipos de objetos distintos, entre ellos la cuenta de usuario.

Generalmente asociada a una persona física, este tipo de objetos permite a dicha persona autenticarse frente a un controlador de dominio. La autenticación se realiza mediante una contraseña que escribe el usuario. Si la autenticación se produce con éxito, se le atribuye al usuario un testigo (token) que contiene su SID (Security IDentifier), único en el dominio AD, así como el conjunto de SID de los grupos a los que pertenece.

Las cuentas de usuario pueden ser locales (se almacenan, en este caso, en una base SAM – Security Account Manager) o de dominio (almacenadas en Active Directory. (Bonnet, 2013)

8.3.6. Políticas de seguridad del Active Directory (GPO)

Un GPO permite implementar configuraciones específicas para uno o varios usuarios y/o equipos. Las GPO permiten administrar objetos de usuarios y equipos, aplicando la más restrictiva en caso de existir más de una política. Se puede usar una GPO para casi cualquier cosa, como indicar que usuario o grupos tiene acceso a una entidad de disco, o limitar el tamaño máximo que puede tener un archivo. (Guijarro, Orozco, Molina, & Trejo, 2018)

Las GPO se pueden diferenciar dependiendo del objeto al que configuran y se pueden entender en distintos niveles.

- Equipo Local: Tan solo se aplican en el equipo que las tiene asignadas independientemente del dominio al que pertenezca.

- Sitio: Se aplican a los equipos y/o usuarios de un sitio, independientemente del dominio.

- Dominio: Se aplican a todos los equipos y/o usuarios de un dominio.
- Unidad Organizativa (OU): Se aplican únicamente a los equipos y/o usuarios que pertenezcan a la OP. (Sierra, 2014)

8.3.7. Servidor DNS

Sistema de nombre de dominio (DNS) es un sistema de bases de datos distribuidas que permite gestionar los nombres de host y las direcciones de Internet (IP) asociadas a ellos.

Con el DNS, la gente puede utilizar nombres simples (como www.jktoys.com) para localizar un host, en lugar de tener que utilizar las direcciones IP (por ejemplo, 192.168.12.88 en IPv4, o 2001: D88::1 en IPv6). Un único servidor solo se puede encargar de conocer los nombres de host y las direcciones IP de una pequeña parte de una zona, pero los servidores DNS pueden colaborar entre sí para correlacionar todos los nombres de dominio con sus direcciones IP. Los servidores DNS que colaboran entre si permiten que los sistemas se comuniquen por Internet. (IBM, 2014)

8.3.7.1. Infraestructura del DNS

La infraestructura del DNS está formada por entidades de procesamiento y comunicación que se encuentran distribuidas. Para entender el funcionamiento del sistema es necesario conocer primero una serie de componentes del mismo, los cuales se definen a continuación: (González, 2015)

- Nombres de dominio

El DNS se basa en un esquema jerárquico de nombres, denominado nombres de dominio. Un nombre de dominio consiste en una secuencia de etiquetas, separadas por puntos, que se leen desde el nodo hasta el root, y que representan hosts individuales que apuntan a una dirección IP. (González, 2015)

- Name Server

Toda la información de un espacio de dominio se guarda en un terminal denominado name server, esto quiere decir que son servidores que almacenan información concreta de una parte del espacio de nombres de dominio, es decir, de una zona, de la que se considera autoritativo. (González, 2015)

- Resource Records o Registro de Recursos (RR)

Una base de datos DNS se compone de uno o varios archivos de zonas. Cada zona se ve definida por un conjunto de recursos denominados Resource o Registro de Recursos (RR).

Estos recursos no siempre tienen que tratarse de una dirección IP, sino que también, entre otras cosas, proporcionan información sobre los alias, el tipo de CPU, el sistema operativo o el name server autoritativo. (González, 2015)

- Resolvers

Cuando los clientes desean acceder a un determinado nombre de dominio utilizan los resolvers como medio para realizar las consultas DNS a los servidores y obtener la información requerida. (González, 2015)

Los resolvers se encargan de:

- Consultar la dirección IP.
- Interpretar las respuestas obtenidas, las cuales pueden ser uno o varios Resource Record, un error de nombre (NE) o un error de búsqueda (Data Not Found).

8.3.8. Servidor DHCP

Un servidor DHCP (Dynamic Host Configuration Protocol) permite a los clientes de una red obtener de forma automatizada una dirección IP que utilizando para gestionar sus comunicaciones en dicha red. El servidor DHCP proporciona al solicitante no solo de una dirección IP, sino que también le proporciona otros ajustes necesarios como pueden ser la puerta de enlace predeterminada a los servidores DNS a utilizar. (Días, Armendáriz, Ruiz, & Castro, 2014)

8.3.8.1. DHCP tiene tres formas distintas de asignar direcciones IP:

- Asignación manual o estática: Distribuye una dirección IP a una máquina determinada. Esto suele ser usado cuando se quiere controlar la asignación de dirección IP a cada cliente y evita que se conecten clientes no autorizados a la red.
- Asignación automática: Esta forma de distribución de direcciones IP es utilizada cuando el número de clientes en la red no varía demasiado. Funciona asignando una dirección IP a una máquina cliente la primera vez que ésta hace la solicitud DHCP al servidor y la misma dirección es asignada cada vez que la máquina se conecta a la red.

- Asignación dinámica: Este método de asignación permite que la dirección asignada a un cliente varía, ya que normalmente una dirección IP es dada al cliente por un intervalo de tiempo. Una vez finalizado el cliente debe volver a hacer la petición para la obtención de una nueva o misma dirección IP. Esto es útil cuando el número de clientes en la red no es fijo. (Cerdán, 2014)

8.3.9. Servidor de Correo Zimbra

El correo electrónico es un servicio de red que permite a los usuarios enviar y recibir mensajes y archivos mediante sistemas de comunicación electrónicos (García, López, & Benavides, 2014).

Un correo electrónico durante su recorrido desde el origen hacia su destino final es procesado por tres agentes, estos son:

Agente de usuario de correo.

Agente de transporte de correo.

Agente de entrega de correo.

El servidor de correo Zimbra es reconocido en varias empresas a nivel del país, como uno de los mejores en mensajería y otros paquetes este incluye en el servicio de correo.

8.3.9.1.Comparación del ciclo de vida del servidor de correo Zimbra

A continuación, veremos las versiones de Zimbra de acuerdo al año de soporte general y de orientación técnica:

Tabla 7. Comparación del ciclo de vida del servidor de correo Zimbra

SERVIDOR DE CORREO ZIMBRA	DISPONIBILIDAD GENERAL	FIN DEL SOPORTE GENERAL	FIN DE LA ORIENTACIÓN TÉCNICA
Versión 8.8	12/12/2017	31/12/2020	31/12/2012
Versión 8.7	13/07/2016	10/09/2019	10/09/2020
Versión 8.6.x	26/08/2015	30/09/2018	30/09/2019
Versión 8.5.x	26/08/2014	30/09/2017	30/09/2018
Versión 8.0	10/09/2012	10/09/2016	10/09/2017

Fuente: (De la Cruz, 2018)

De acuerdo a la versión que ha evolucionado el servidor de correo Zimbra, dentro de estos tenemos los más principales según cada característica que las definen.

Zimbra 8.6.x

Fuera de la orientación técnica, ya desde septiembre de 2018 no se lazaba ningún nuevo parche ni se corregían los errores en esta versión (De la cruz, 2020).

Zimbra 8.7.11

La versión más robusta y severas que Zimbra ha sufrido se queda sin soporte general y entra en orientación técnica, lo que significa que no veremos más errores resueltos ni parches (De la cruz, 2020).

Zimbra 8.8.12

Se queda sin soporte general y entra en orientación técnica, lo que significa que no veremos más errores resueltos ni parches (De la cruz, 2020).

Según las comparaciones de cada versión del Zimbra, la que se ha utilizado en este proyecto de investigación ha sido la versión 8.8.12, la cual ha funcionado a la perfección sin ningún problema, dando como resultados positivos en lo que respecta a la práctica realizada para este proyecto.

9. VALIDACIÓN DE LAS PREGUNTAS CIENTÍFICAS:

Si el GAD Municipal del Cantón Mejía contara con un servidor de dominio, mediante la administración de cuentas de seguridad, ayudaría a garantizar el acceso a recursos y servicios dando como resultado un mejor acceso de las personas en la red.

Tabla 8. Descripción de variables.

VARIABLES	CONTENIDO DE LA PREGUNTA
Variable dependiente	Garantizar el acceso a recursos y servicios de los usuarios en la red.
Variable independiente	Servidor de dominio

Fuente: Grupo investigador.

10. METODOLOGÍAS Y DISEÑO EXPERIMENTAL

10.1. Materiales

En el desarrollo de este proyecto de investigación, se hizo uso de diferentes materiales, métodos, técnicas y los diferentes tipos de metodologías, los que nos permitieron la redacción y acopio de información necesaria para el desarrollo del proyecto de investigación, esto se detallan a continuación:

10.1.1. Materiales Bibliográficos

- Libros
- Internet
- Folletos
- Artículos Científicos
- Libros virtuales
- Tesis
- Enciclopedias
- Bases de datos

Estos son las principales fuentes de consultas, permitiéndonos así la obtención de muchos conocimientos claros y precisos, que nos sirven para argumentar el proyecto de titulación.

10.1.2. Equipos Informáticos

- Disco duro portable
- Router
- Flash Memory
- PC´s
- Laptop
- Servidor
- Switch
- Access Point

En el desarrollo del proyecto de titulación se pueden hacer uso de diversos equipos informáticos, para el desarrollo del Active Directory.

10.2. Métodos

Los principales métodos aplicados en el desarrollo del proyecto de investigación, son los siguiente:

10.2.1. Método analítico

A partir del conocimiento general de una realidad realiza la distinción, conocimiento y clasificación de los distintos elementos esenciales que forman parte de ella y de las interrelaciones que sostienen entre sí. Se fundamenta en la premisa de que a partir del todo absoluto se puede conocer y explicar las características de cada una de sus partes y de las relaciones entre ellas. (Abreu, 2014)

Como podemos observar el método analito nos fue de gran utilidad ya que pudimos analizar nuestra problemática, visualizando de manera minuciosa los inconvenientes, consecuencias y causas que trae la instalación del active directory.

10.2.2. Método científico

El método científico es el camino para producir conocimiento objetivo, es un modo razonado de indagación establecido en forma deliberada y sistemática, que está constituido por una serie de etapas o pasos para producir conocimientos. (Asuad, 2014)

El método científico es de vital importancia, ya que con este método pudimos realizar la recolección de conocimientos teóricos para el desarrollo del proyecto de titulación.

10.3. Técnica

La principal técnica usada en el desarrollo de la investigación se describe a continuación:

10.3.1. Técnica de Observación

La observación es uno de las técnicas que permiten la recolección de información que consiste en contemplar sistemática y detenidamente como se desarrolla la vida de un objeto social. Alude, por tanto, al conjunto de ítems establecida para la observación directa de sucesos que ocurren de un modo natural. Esta definición implica dos consideraciones principales: en primer lugar, que los datos se recogen cuando ocurre el suceso, sin que ello implique la imposibilidad de que sea grabado o recogido para su posterior análisis; en segundo lugar, significa que el suceso no es creado, mantenido o finalizado exclusivamente para la investigación, ya que entonces estaríamos hablando del denominado método experimental. (Pulido, 2015)

Esta técnica nos ayudó a tener una perspectiva clara de los problemas que existen en el GAD Municipal del Cantón Mejía, poniendo como principal problema la seguridad de la red de datos, para poder centralizar los recursos y servicios que existe en el GAD.

10.4. Metodología

10.4.1. Metodología Científica

La metodología científica tiene la finalidad de comprender el proceso de investigación que se realiza al momento de cualquier investigación y no los resultados de la misma. Se pueden tener tantas metodologías como diferentes formas y maneras de adquirir conocimientos científicos del saber común que se denomina "ordinario", las cuales responden de distinta manera a cada una de las preguntas y cuestionamientos que se plantea la propia metodología. (Maya, 2014)

10.4.2. Tipos de investigación

10.4.2.1. Investigación Bibliográfica

La investigación documental o bibliográfica, se caracteriza por la utilización de documentos; que permiten obtener resultados coherentes; porque utiliza los procedimientos lógicos y mentales de toda investigación; análisis, síntesis, deducción, inducción, etc. Porque realiza un proceso de abstracción científica, generalizando sobre la base de lo fundamental; porque supone una recopilación adecuada de datos que permiten redescubrir hechos, sugerir problemas, orientar hacia otras fuentes de investigación. (Rodríguez, 2013)

La investigación bibliográfica permite, entre otras cosas, apoyar la investigación que se desea realizar, evitar emprender investigaciones ya realizadas, tomar conocimientos de experimentos ya hechos para repetirlos cuando sea necesario, continuar investigaciones interrumpidas o incompletas, buscar información sugerente, seleccionar los materiales para un marco teórico. (Rodríguez, 2013)

10.4.2.2. Investigación Mixta

Para nuestro proyecto de titulación se utilizó la investigación mixta la que entremezclan la investigación cualitativa como cuantitativa, las mismas que nos van a permitir a recolectar, analizar y vincular información sobre el desarrollo de un servidor de dominio, la cual nos permitió obtener una mejor exploración y aprovechamiento de información que fueron analizados para alcanzar resultados satisfactorios. (Ruiz M. , 2013)

10.5. Diseño Experimental

En el diseño Experimental vamos a Diseñar, planificar e implementar.

10.5.1. Diseño

Para la realización de este proyecto se planea realizar el diseño físico o lógico de cómo se encuentra estructurado el servidor de dominio basado en los requerimientos del administrador, los cuales tenemos como prioritario la configuración de los servidores DNS, DHCP y el servidor de DOMINIO con toda la infraestructura de los grupos organizacionales en una manera jerárquica y ordenada por departamentos, así como la configuración de equipos, usuarios, cableado y conexiones a la red.

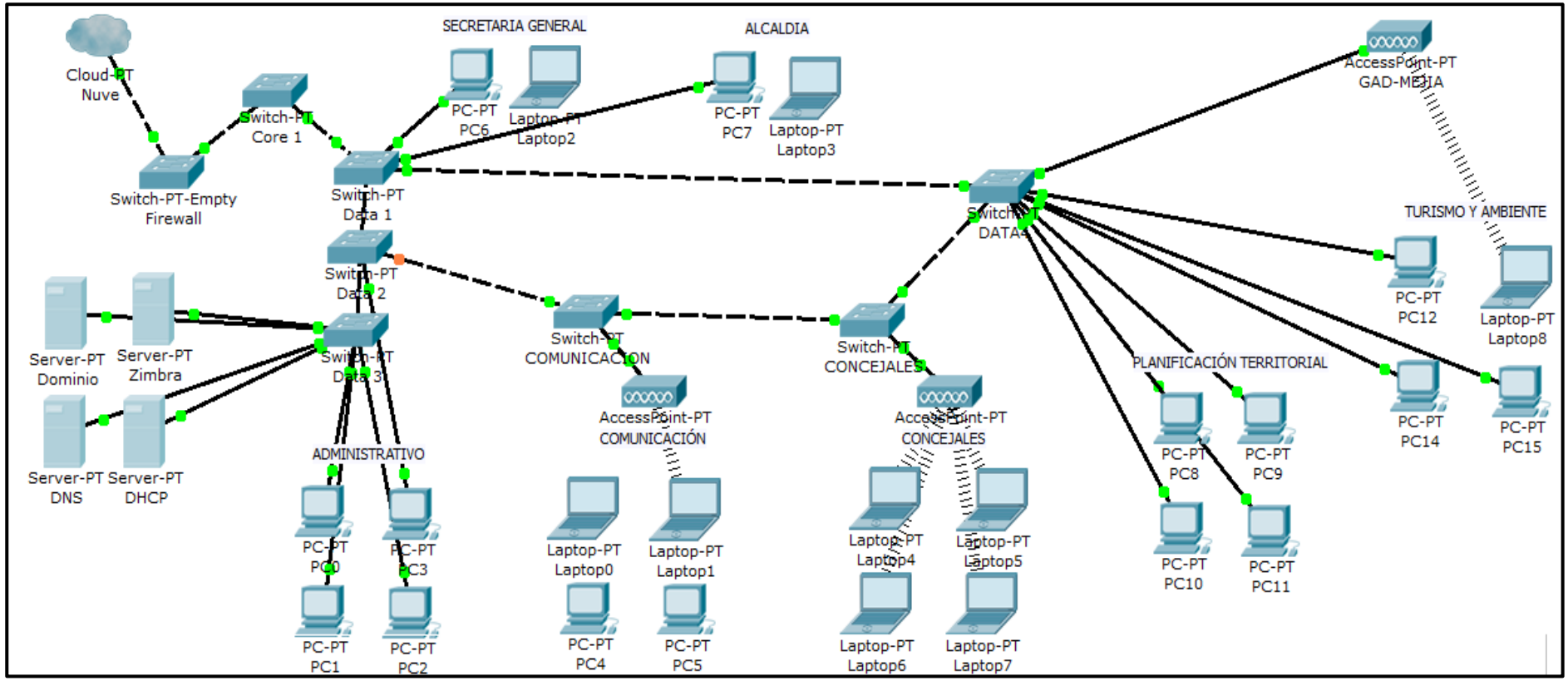
10.5.1.1. Topología

Vamos a describir la topología que el GAD Municipal del Cantón Mejía usa de acuerdo a sus protocolos y estándares, es una topología combinada que toma su nombre como mixta su creación y su nombre se da por la unión de los diferentes tipos de topologías, en nuestro caso para nuestro proyecto encontramos que es una topología anillo-estrella dado que los equipos están conectados a un switch HP s200cs con topología estrella. Sin embargo, estos switch están conectados con una topología en anillo con los diferente switch que cada edificio tiene, con esta topología aseguramos redundancia en la red para garantizar la comunicación de datos en un 99.9%.

10.5.1.2. Tipo de clase

El GAD Municipal del Cantón Mejía en su infraestructura y configuración trabaja con redes de clase C en el rango 192. y con una máscara de 255.255.255.0 las cual está compuesta por vlans que están configurados para los departamentos de acuerdo a su ubicación porque nos proporciona varias ventajas como la simplificación de administración de la red, flexibilidad, escalabilidad, seguridad, adicional se cuenta también con vlans para teléfonos, impresoras, cámaras y equipos biométricos dándonos un total de 38 vlans.

Figura 6. Diseño del servidor de dominio.



Fuente: Grupo Investigador

10.5.2. Planificación

10.5.2.1. Servidores

Para la planificación de este proyecto del servidor de dominio, mediante Security Account Manager por requerimiento especifico del administrador de data center contaremos con un entorno Windows server 2012 R2 debido a que se otorgara la licencia por parte de la institución y en el cual se levantara los servicios de control de dominio, con Windows Server 2012 R2 nosotros podremos realizar la configuración de varios servicios, los cuales fueron desarrollados para facilitar la administración centralizada de los recursos y usuarios pertenecientes al GAD Municipal de Mejía

Para la investigación mediante la observación y la entrevista al administrador del Data Center, redes y telecomunicaciones nos proporciona los requisitos, requerimientos y datos para la configuración y la estructura del servidor de dominio el cual uno de los requisitos es que lleve como nombre de equipo MEJIA-AD, el nombre de dominio será **municipiomejia.gob,** también la respectiva dirección IP para el servidor, el nombre de usuario y password.

10.5.2.2. Unidades Organizativas

Se planifica con el administrador del data center en crear unas unidades organizativas como: raíz tendremos de nombre al GADMUNICIPALMEJIA, de esta carpeta creada se van a crear 3 categorías que son: Usuarios, Equipos y Grupos, en las cuales se establecieron que en los Usuarios vamos a ingresar todos los departamentos que posee la institución y dentro de ellos crear los usuarios que correspondan a dicho departamento, la categoría Equipos van a ingresar todas las computadoras y laptop que ingresemos al dominio, en este caso a los equipos les nombraremos de la siguiente manera GAD-TH-LAP01, ya cuando estén dentro del dominio vamos a poner el nombre de la persona que la está utilizando, para poder tener un mejor control de los equipos, y en la Categoría Grupos vamos a dividirlos en dos las cuales son personas comunes y no comunes.

Las personas comunes se refieren a que puede tener acceso a todo el manejo del equipo panel de control y permitir que se descarguen e instalan cualquier sistema sin la necesidad de llamar al servicio técnico de TIC´s.

Las personas no comunes se refieren que ellos no tienen los privilegios de nada que no pueden ni descargar ni instalar algún programa y que deben solicitar al departamento de TIC´s para cualquier instalación.

10.5.2.3. Políticas GPO

Para la planificación de las políticas, se quedó con el administrador del data center en crear las más esenciales las cuales son: Mensaje de bienvenida, Fondo de pantalla, Contraseñas incorrectas, Caducidad de contraseña y la inactividad del tiempo. Pero dependiendo a que categoría pertenece o se basa la política.

Las políticas GPO son reglas que nos permiten controlar el entorno de trabajo de las cuentas de usuarios y las cuentas de los equipos.

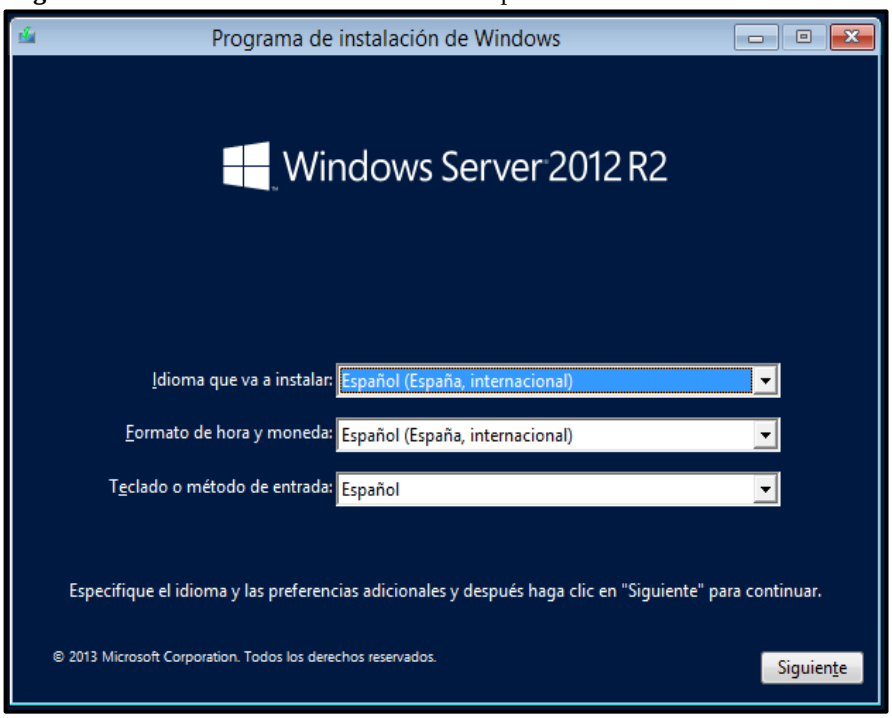
10.5.3. Implementación

Windows Server 2012 R2 nos permite la configuración de varios servicios, que están desarrollados para facilitar la administración a los usuarios, ya que existen muchas ediciones las cuales son optimizadas y simplificadas para que los usuarios puedan elegir la edición que más les convenga de acuerdo a las necesidades que posee las empresas e instituciones.

Para la implementación del Active Directory vamos a empezar por la instalación del sistema operativo Windows Server 2012 R2.

1. Como podemos ver en la Figura 7. Vamos a empezar con la instalación del Sistema Operativo Windows Server 2012 R2. Y para eso debemos escoger cual es el idioma al que va a ser instalado.

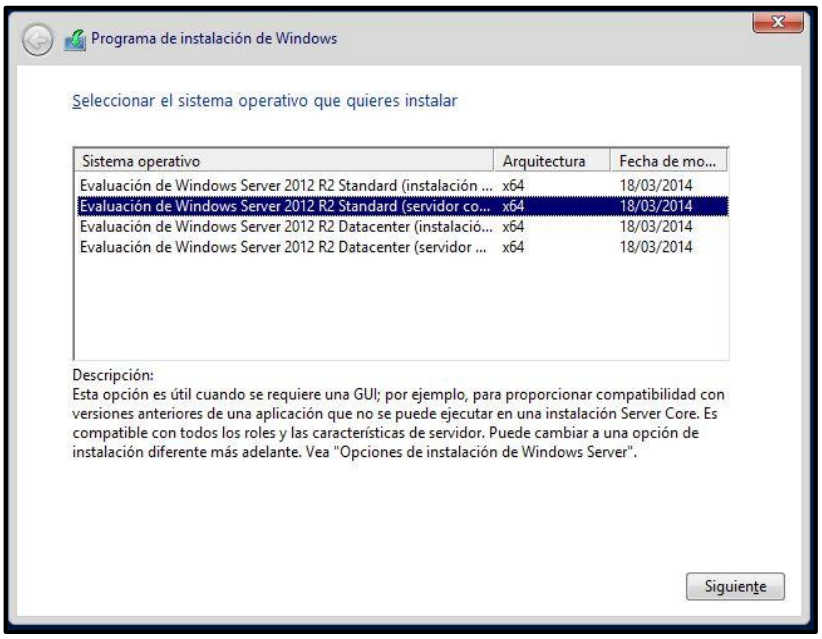
Figura 7. Selección del Idioma del Sistema Operativo.



Fuente: Grupo investigador.

2. Seleccionamos la versión a instalar como lo vemos en la figura 8, el cual para este proyecto de investigación se escogió Windows Server 2012 R2 Standard, con una arquitectura de 64.

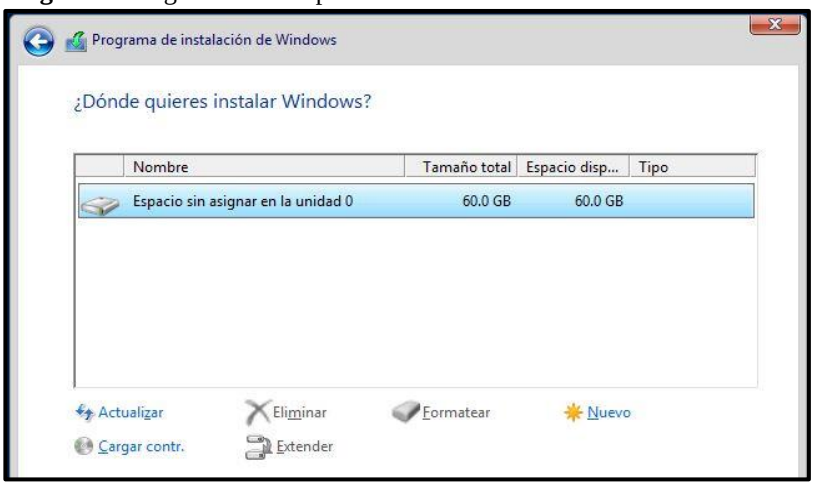
Figura 8. Selección del sistema operativo.



Fuente: Grupo investigador

3. En la figura 9, vamos a poder asignar el espacio en la Unidad C del sistema operativo.

Figura 9. Asignación del espacio en la unidad C.



Fuente: Grupo investigador.

4. Como podemos observar en la figura 10, el proceso final de la instalación del Sistema Operativo Windows Server 2012 R2. En donde se están instalando los respectivos drivers, archivos del sistema, actualizaciones y configuraciones para su primer uso y que nos funcione de una forma adecuada.

Figura 10. Instalación de los respectivos drivers de Windows Server.

Fuente: Grupo investigador.

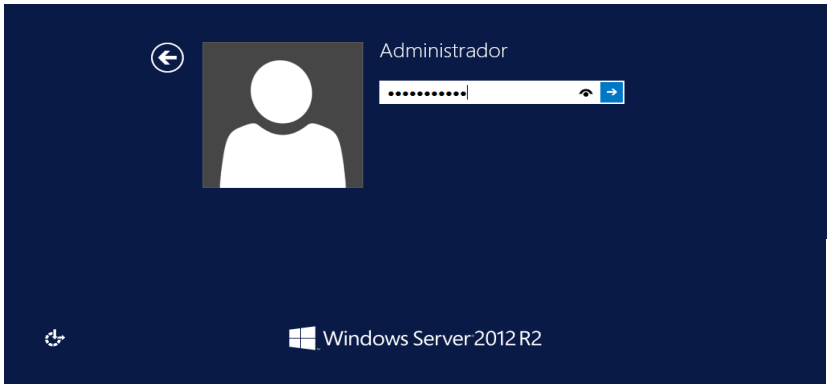
5. Una vez acabado la instalación de los drivers, procedemos a introducir una contraseña, como lo vemos en la figura 11, en donde finalizará la instalación de Windows Server y después se procederá a la instalación y configuración del Servidor de Dominio.

Figura 11. Introducción de contraseña.

Fuente: Grupo investigador.

6. Una vez que se acabe de actualizar nos va a aparecer el nombre que en este caso es Administrador y que presionemos las teclas CTRL + ALT + SUPR, para poder ingresar la clave y de inmediato ingresa a la pantalla principal de Windows Server 2012 R2. Como lo podemos observar en la figura 12.

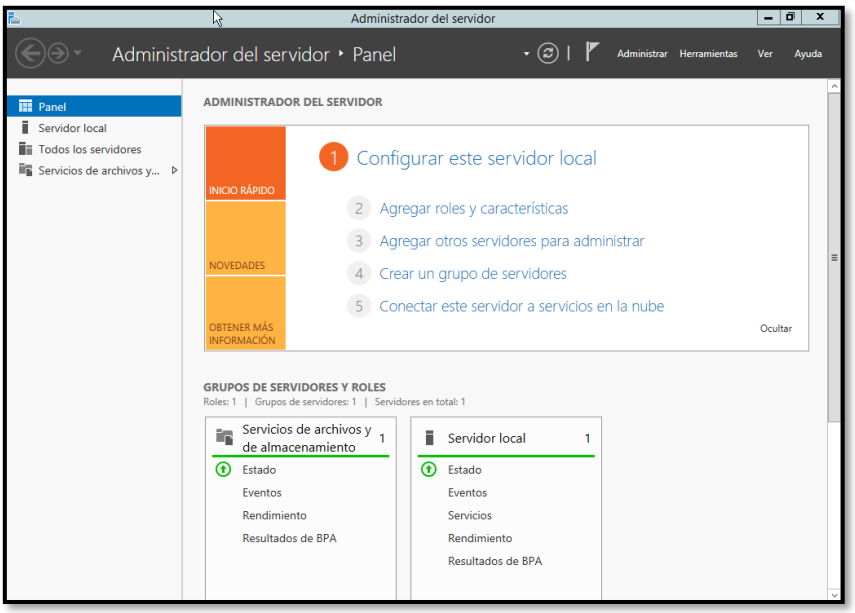
Figura 12. Ingreso a Windows Server 2012.



Fuente: Grupo investigador

7. En la figura 13. Podemos observar la pantalla principal de Windows Server 2012 R2. El cuál es el administrador del servidor.

Figura 13. Administrador del servidor.

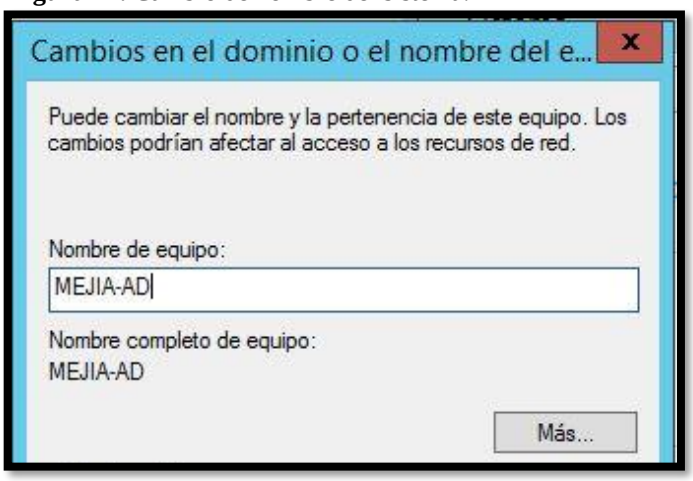


Fuente: Grupo investigador.

10.5.3.1. Instalación del servicio del Active Directory.

1. Al momento de haber ingresado a Windows 2012 R2, como podemos ver en la figura 14, vamos a configurar el nombre de la máquina, para eso seguimos estos pasos: ingresamos a Mi PC, propiedades, cambiar configuración, esto nos sirve para poder configurar el servidor de dominio de una mejor manera.

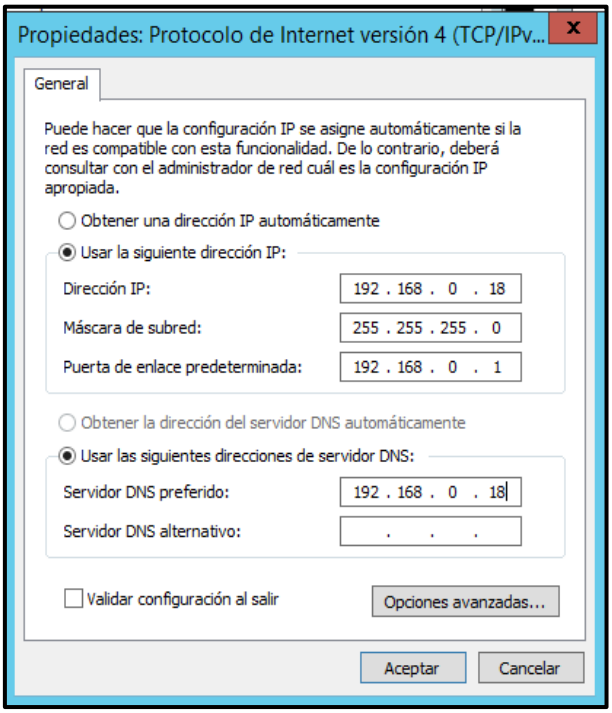
Figura 14. Cambio de nombre del sistema.



Fuente: Grupo investigador

2. Como podemos observar en la figura 15, vamos a asignar una dirección IP estática, teniendo en cuenta que debemos ingresar de igual manera a un servidor DNS y este será el mismo que ingresamos en la dirección IP.

Figura 15. Configuración de una dirección IP estática.



Fuente: Grupo investigador

3. Al momento de tener configurado la dirección IP, nos dirigimos a la pestaña de administración del servidor y seleccionamos la opción “Agregar roles y características”, como lo vemos en la figura 16, con esto nos apareceré una ventana preguntando qué tipo de instalación vamos a realizar, escogemos la opción de “instalación basada en características o roles” y pasamos al siguiente ítem.

Figura 16. Selección del tipo de instalación.

Fuente: Grupo investigador

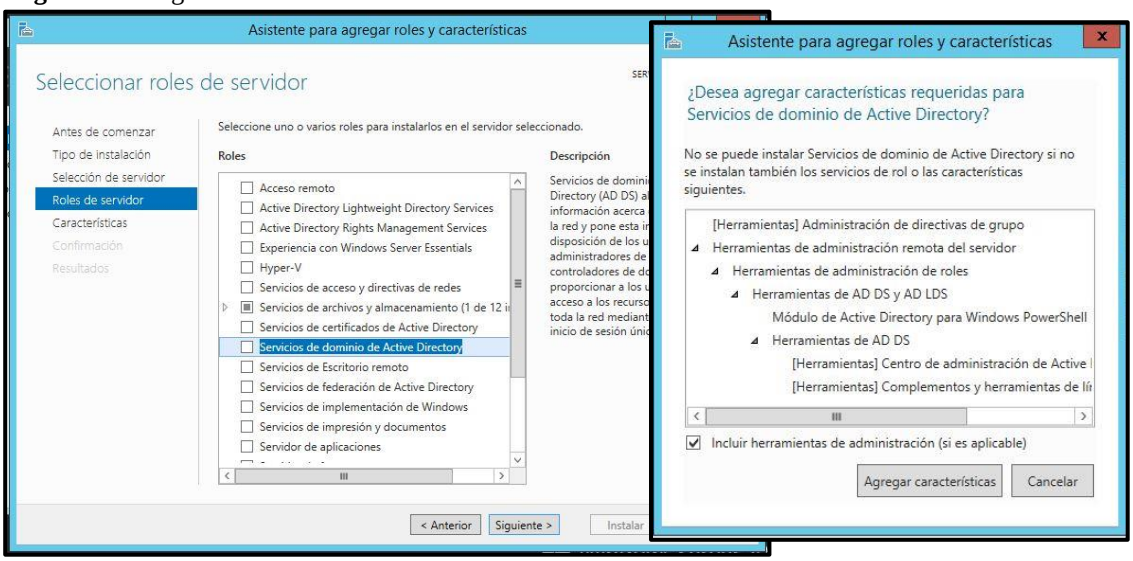
4. Una vez seleccionado el tipo de instalación, debemos seleccionar el servidor de destino, podemos verlo en la figura 17. Teniendo en cuenta que debemos aplicar el ítem: "Seleccionar un servidor del grupo de servidores", en ese momento aparecerá el nombre del equipo y la dirección IP ya que configuramos al inicio cuando ya habíamos instalado Windows Server 2012 R2.

Figura 17. Selección del servidor.

Fuente: Grupo investigador

5. Continuamos agregando los roles al servidor, para ello seleccionamos el ítem: Servicios de dominio de Active Directory, se desplegará una ventana emergente, en el cual indica las características a ser instaladas, como se muestra en la figura 18, en donde se debe seleccionar "agregar características" para continuar con la instalación.

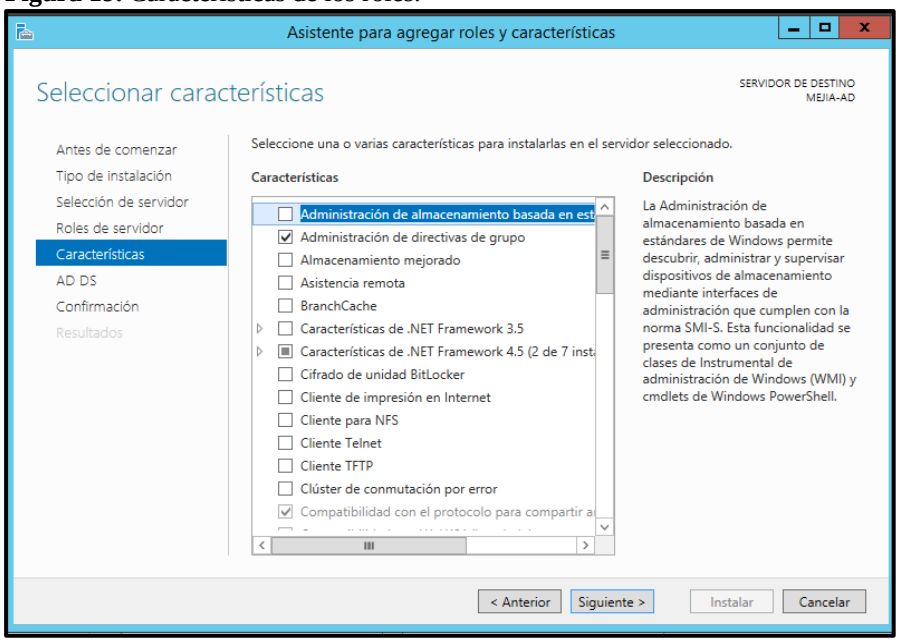
Figura 18. Asignar roles del servidor.



Fuente: Grupo investigador.

6. Al hacer clic en Agregar características, podemos visualizar que las características del DNS ya se encuentran instaladas correctamente, como se puede visualizar en la figura 19.

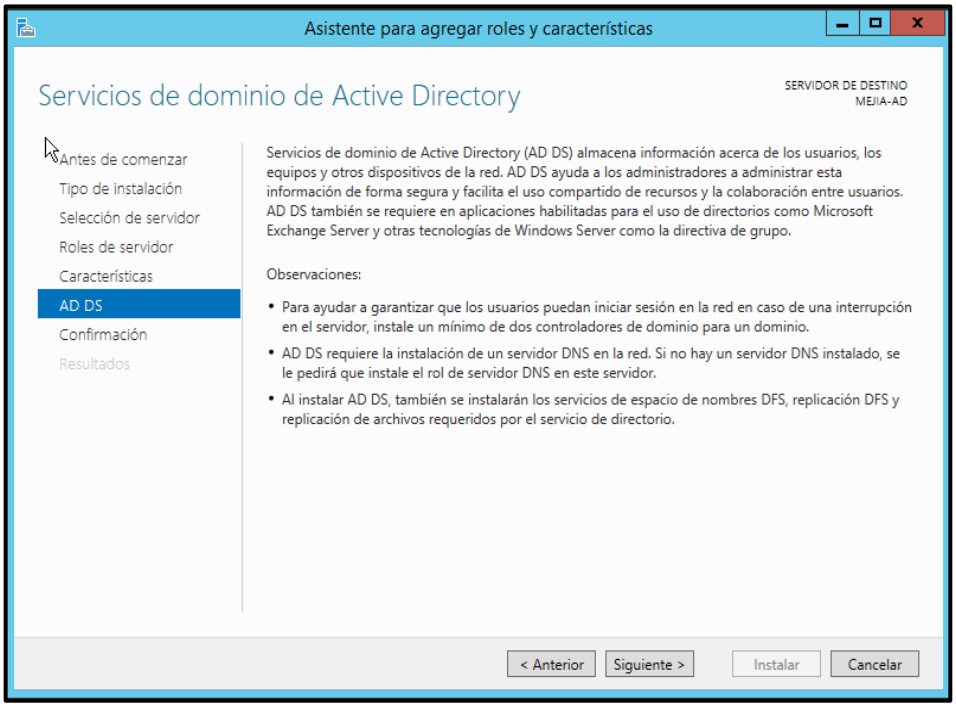
Figura 19. Características de los roles.



Fuente: Grupo investigador.

7. La figura 20, muestra información acerca de los servicios del directorio activo, lo único que se realiza aquí es dar clic en “Siguiente”.

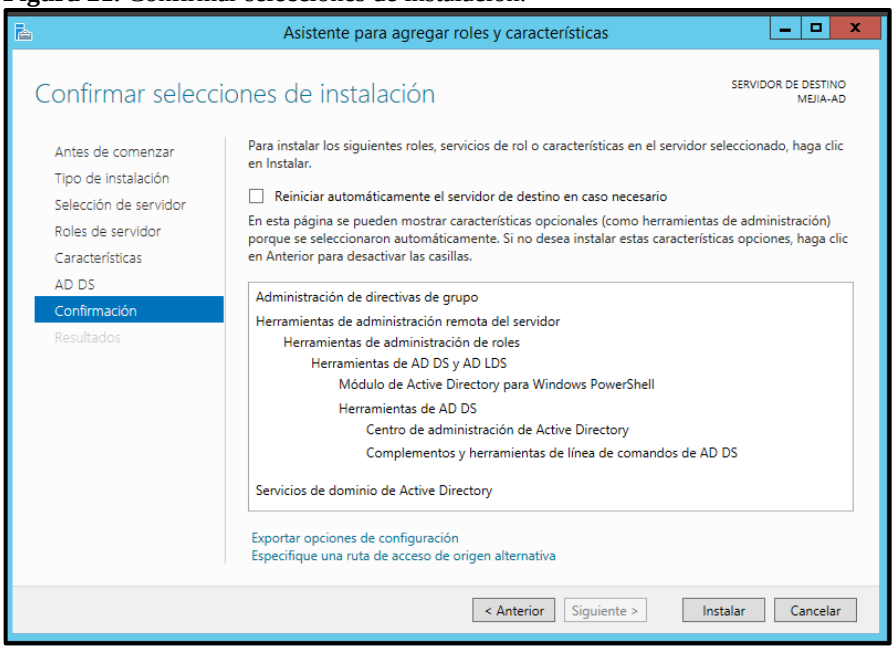
Figura 20. Información y observaciones del servicio de dominio.



Fuente: Grupo investigador.

8. La ventana de confirmar “selecciones de instalación”, muestra las características que instalar en el servidor, para continuar con la instalación, se da clic en “Instalar” como indica en la figura 21.

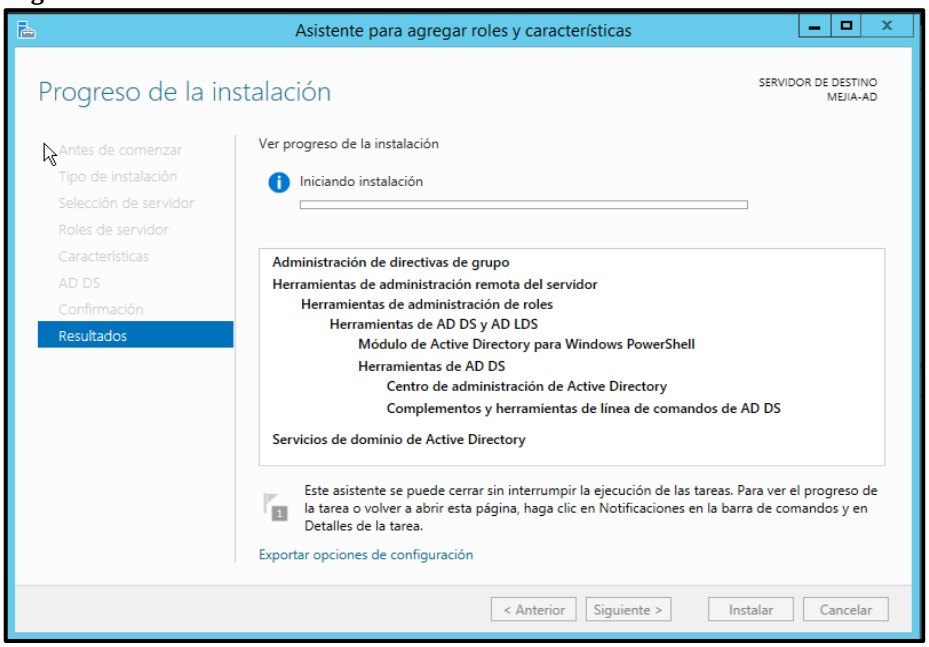
Figura 21. Confirmar selecciones de instalación.



Fuente: Grupo investigador.

9. Al momento de dar clic en “Instalar” en la figura 21, se muestra la siguiente pantalla que es el “proceso de instalación” como se detalla en la figura 22, aquí debemos esperar un momento hasta que se culmine.

Figura 22. Proceso de instalación.

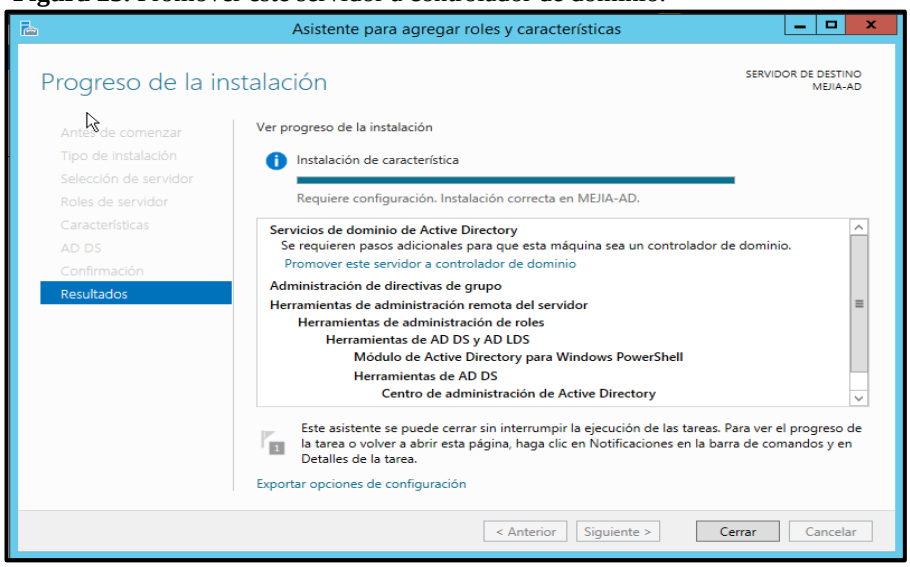


Fuente: Grupo investigador.

10.5.3.2. Instalación del Controlador de dominio.

1. Una vez finalizada la instalación como podemos observar en la figura 23, antes de cerrar debemos configurar el siguiente ítem "Promover este servidor a controlador de dominio".

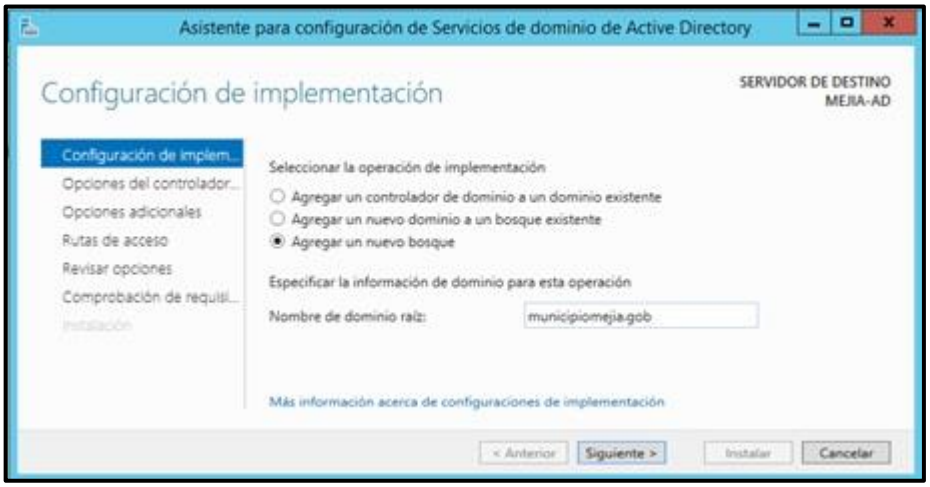
Figura 23. Promover este servidor a controlador de dominio.



Fuente: Grupo investigador.

2. En la primera ventana de configuración se marcará la opción "Agregar un bosque", y ahí debemos ingresar el nombre del dominio raíz, en este caso municipiomejia.gob, y dar clic en siguiente, como se puede observar en la figura 24.

Figura 24. Configuración de implementación.

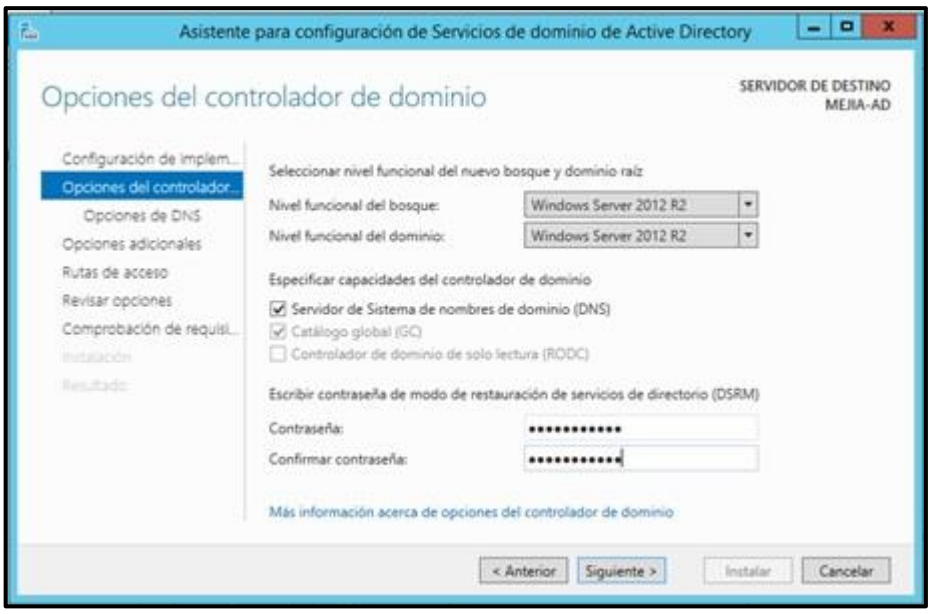


Fuente: Grupo investigador.

3. En la pantalla de "opciones de controlador de dominio", se debe asegurar que el nivel funcional del bosque y del dominio, sea Windows Server 2012, en capacidades del controlador de dominio viene por defecto marcado el ítem Catalogo Global, la razón de

esto es que es el primer controlador del dominio, por último, se establece la contraseña que va a tener el servicio de directorio, como se muestra en la figura 25.

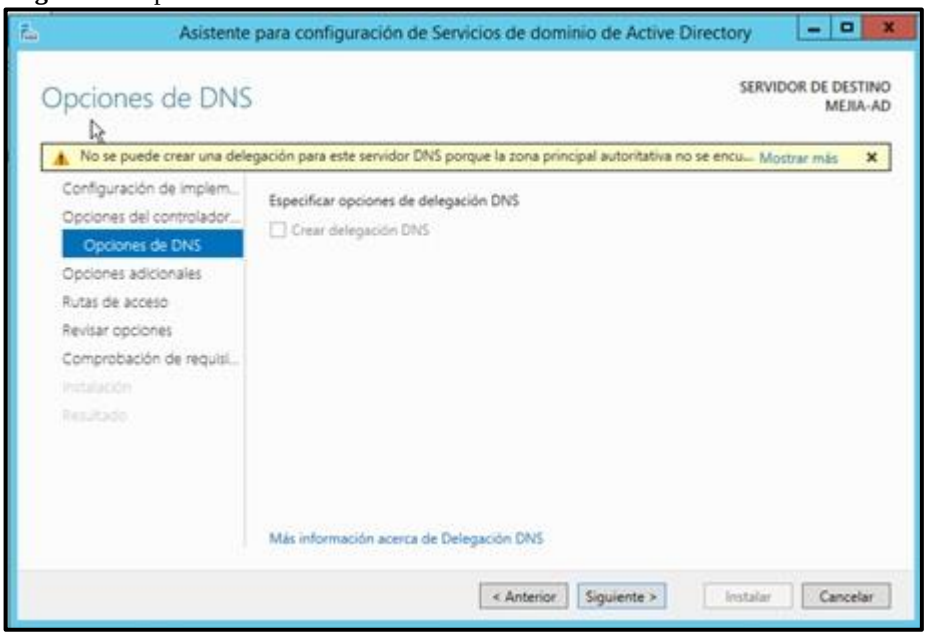
Figura 25. Opciones del controlador de dominio.



Fuente: Grupo investigador.

4. En la opción DNS simplemente se da clic en Siguiente, para continuar con la configuración, como se observa en la figura 26.

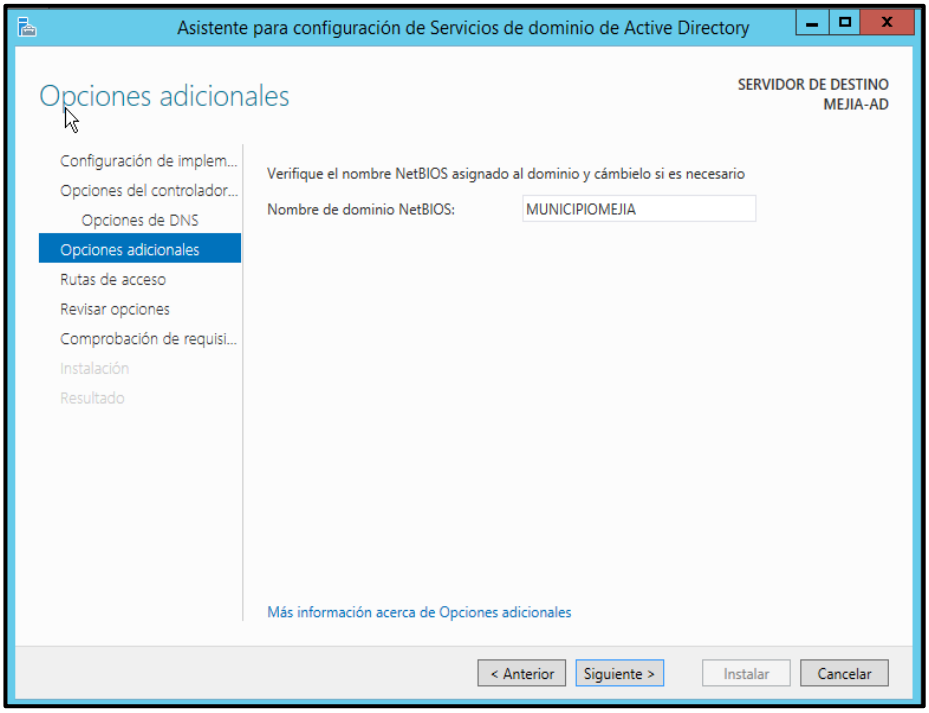
Figura 26. Opciones DNS.



Fuente: Grupo investigador.

5. En la figura 27, se valida el nombre de dominio NetBIOS y se procede a poner en la opción siguiente.

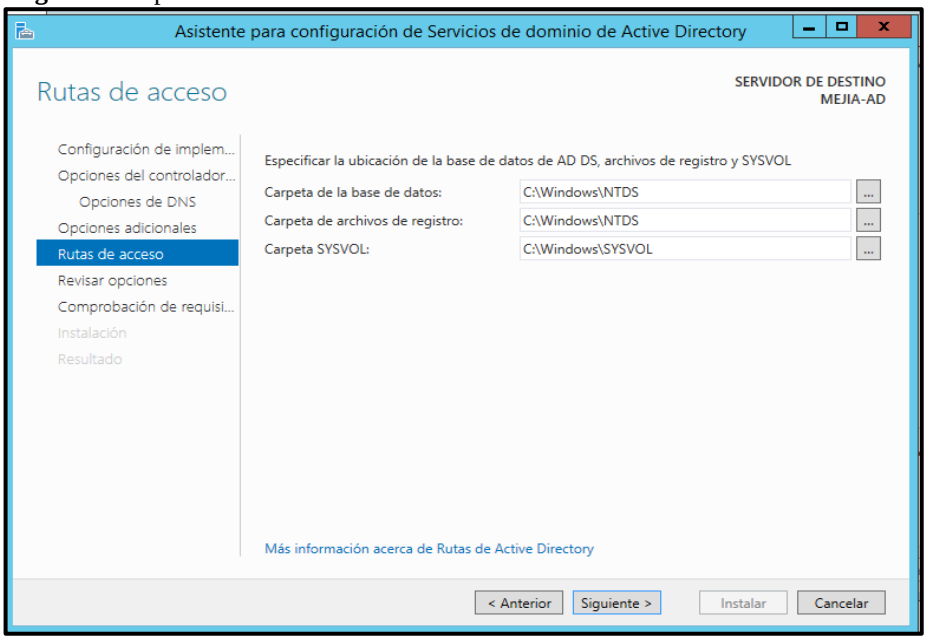
Figura 27. Nombre de dominio NetBIOS.



Fuente: Grupo investigador.

6. En la figura 28, se definen las rutas de las carpetas de la base de datos de ADDS.

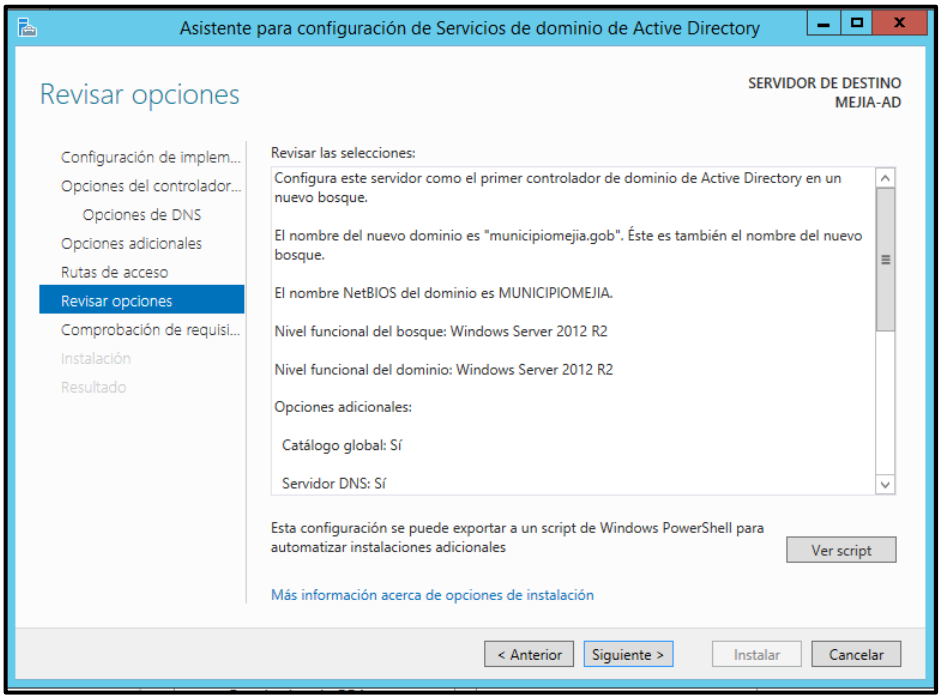
Figura 28. Opciones adicionales.



Fuente: Grupo investigador.

7. En la ventana revisar opciones, muestra las características principales: como el nombre de dominio, nombre de NetBIOS y los niveles funcionales. Esto se describe en la figura 29.

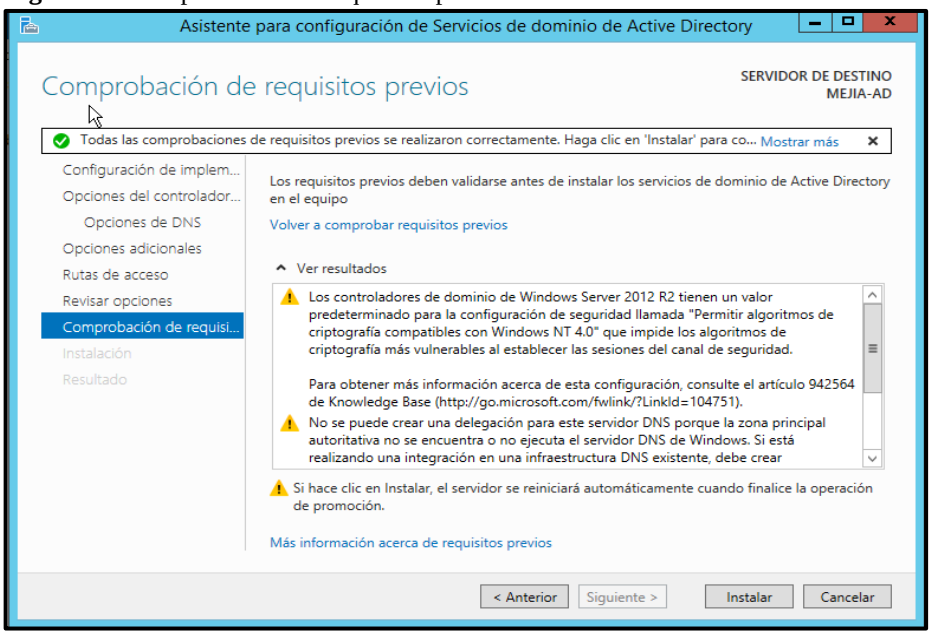
Figura 29. Revisar opciones.



Fuente: Grupo investigador.

8. Cuando hayamos puesto en la opción "siguiente" nos aparecerá la pantalla de comprobación de requisitos previos, una vez que haya realizado una comprobación de manera exitosa, como se muestra en la figura 30, se da clic en "Instalar."

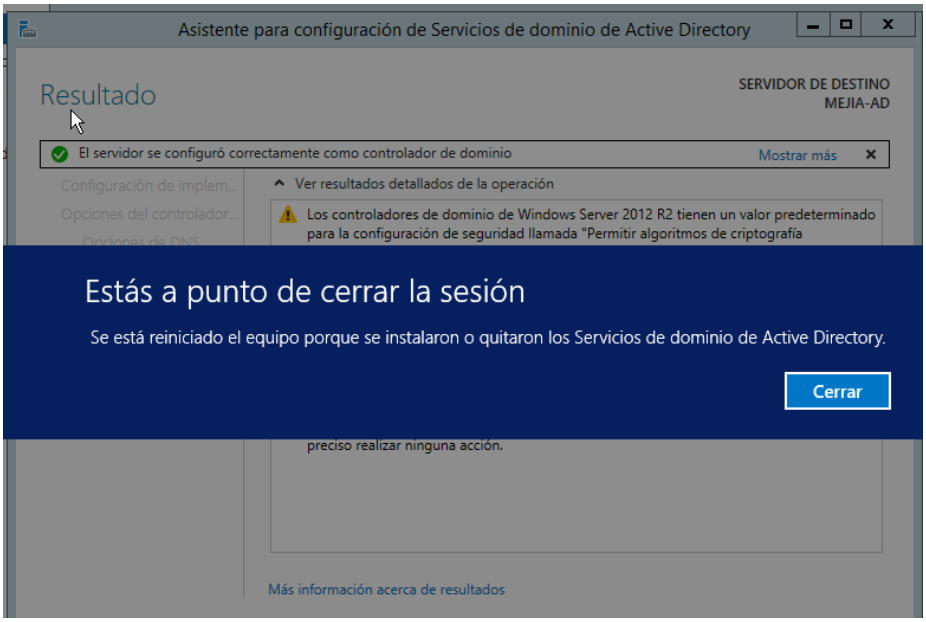
Figura 30. Comprobación de requisitos previos.



Fuente: Grupo investigador.

9. Al culminar la instalación el equipo automáticamente se reinicia, podemos verlo en la figura 31.

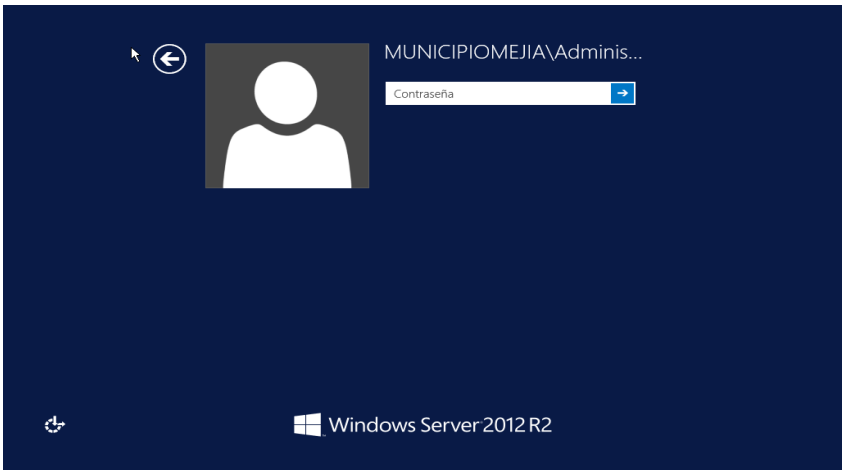
Figura 31. Reinicio automático del sistema.



Fuente: Grupo investigador.

10. En la figura 32, podemos observar que al momento que se reinicia el sistema operativo se realiza el cambio del usuario al momento que se ingresa nos aparece con el nombre del dominio DNS que hemos creado satisfactoriamente.

Figura 32. Ingreso al sistema Windows Server 2012 con el DNS.



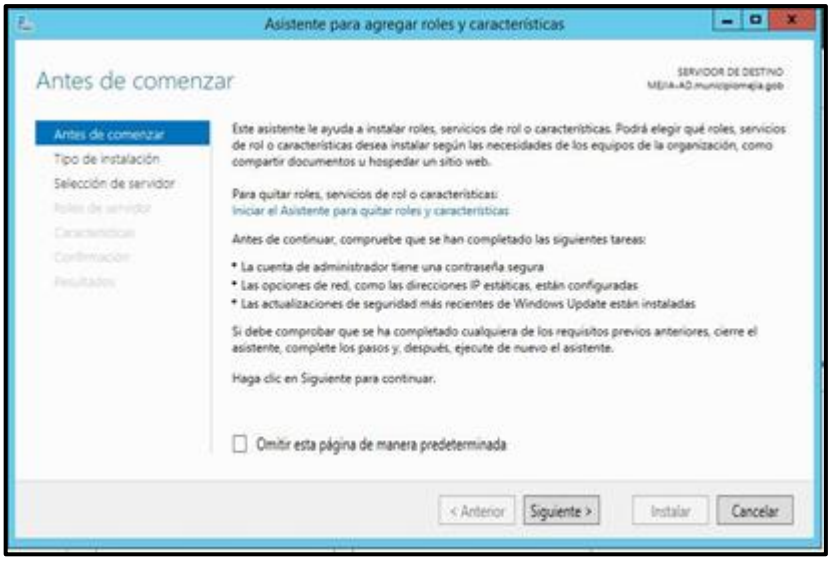
Fuente: Grupo investigador.

10.5.3.3. Instalación del servicio DHCP

Una vez ya instalado el controlador del dominio comenzamos con la configuración del controlador DHCP y por eso vamos a seguir los siguientes pasos.

1. Para el controlador del DHCP, escogemos casi las mismas opciones que al momento de configurar el DNS, elegimos la opción roles y características, nos aparece la primera ventana el cual nos muestra en la figura 33.

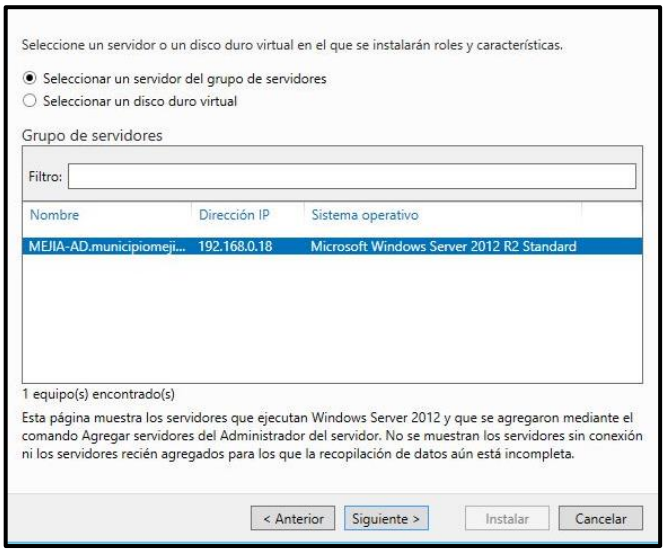
Figura 33 . Asistente de roles y características.



Fuente: Grupo investigador.

2. Después de seleccionar el tipo de instalación, vamos a seleccionar “siguiente”, nos aparece otra pantalla en donde una vez seleccionado el tipo de investigación, tenemos que seleccionar el servidor de dominio y verificar que los datos estén bien, como se observa en la figura 34.

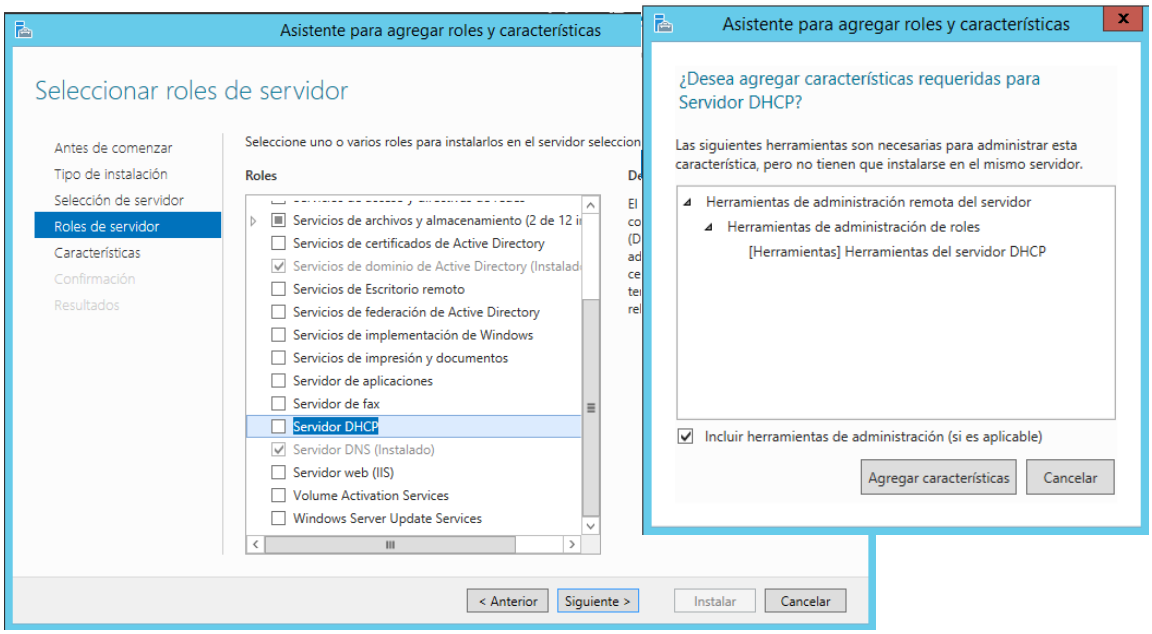
Figura 34. Servidor de destino del DHCP.



Fuente: Grupo investigador.

3. En la figura 35, vamos a observar la pantalla de seleccionar roles del servidor, para ello seleccionamos el ítem “Servicio DHCP”, y junto con eso agregamos las características que posee el DHCP.

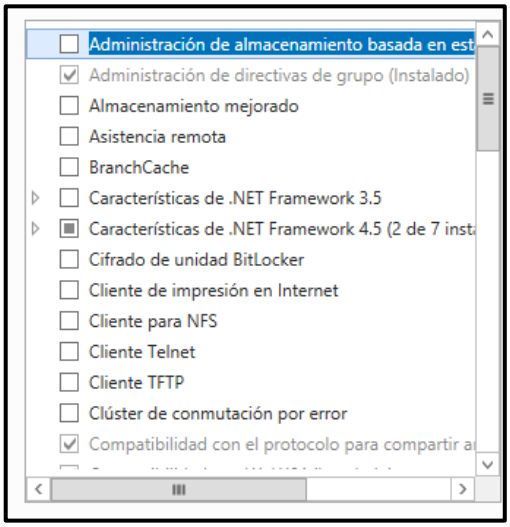
Figura 35. Instalación del servidor DHCP y características.



Fuente: Grupo investigador.

4. Al momento de haber agregado el servicio DHCP y las características, vamos a observar en la figura 36, las características que se instalaron por defecto junto al servicio DHCP, y lo único que hacemos es poner en “siguiente”.

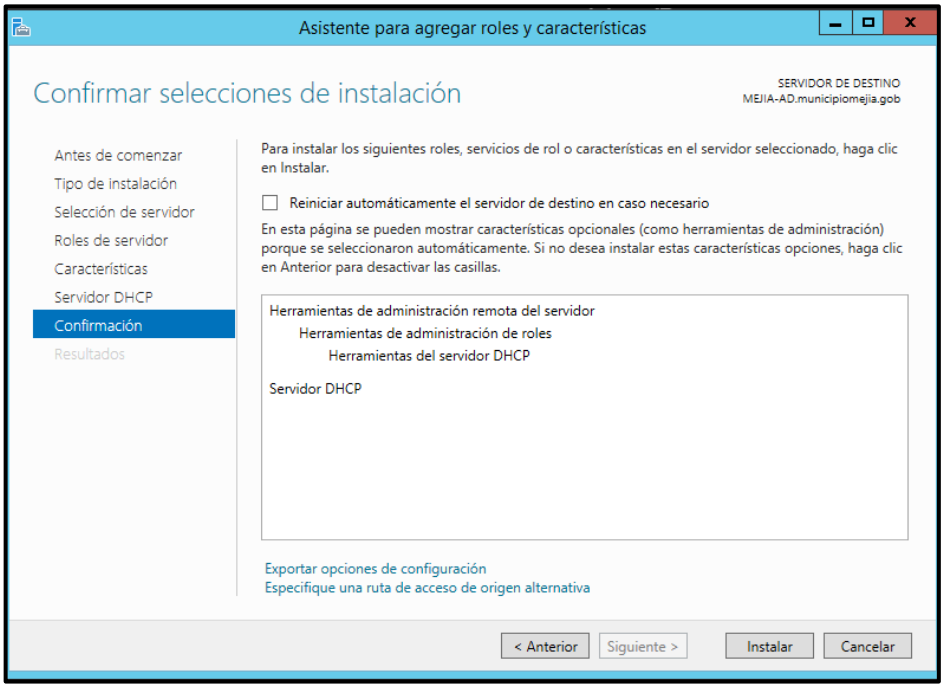
Figura 36. Seleccionar características del DHCP.



Fuente: Grupo investigador.

5. En la figura 37, vamos a confirmar la instalación del servidor DHCP, lo siguiente que debemos hacer es poner en el ítem “Instalar”.

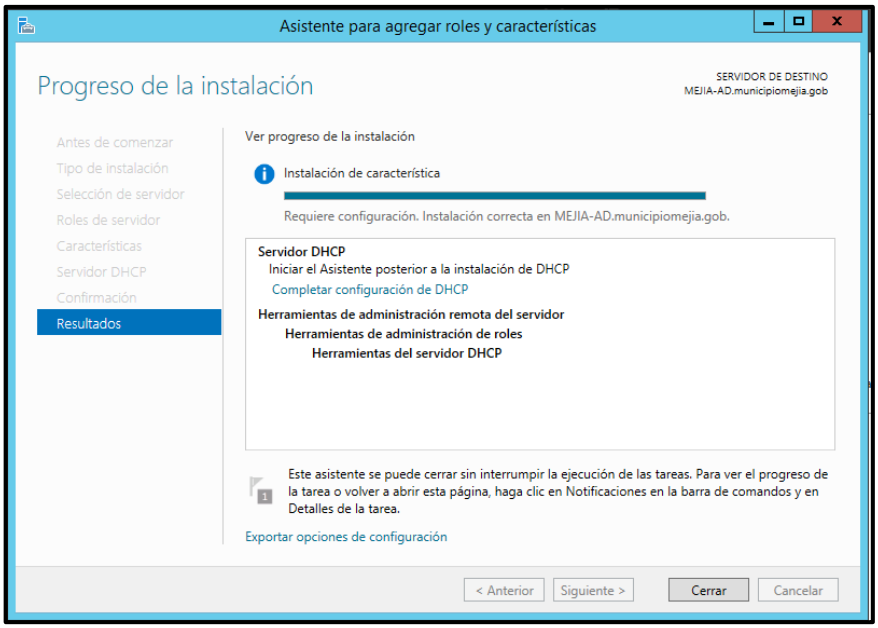
Figura 37. Confirmación de la instalación del servidor DHCP.



Fuente: Grupo investigador.

6. Una vez que culmine la instalación, vamos al ítem "Completar configuración de DHCP", como lo podemos ver en la figura 38.

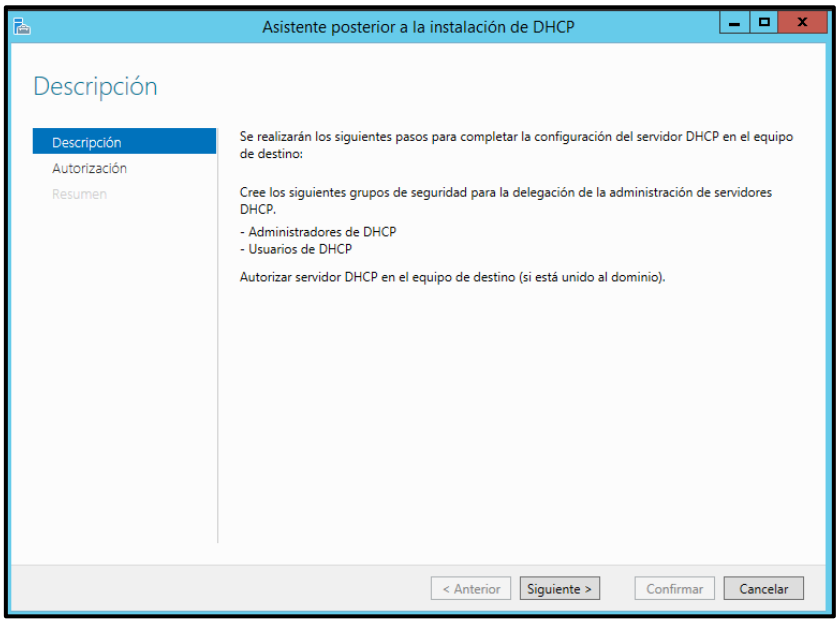
Figura 38. Progreso de la instalación del servicio DHCP.



Fuente: Grupo investigador.

7. En la figura 39 vemos que aparece una pantalla en donde nos va a aparecer una descripción del servicio del DHCP, lo único que aquí se hace es poner en la opción "Siguiente".

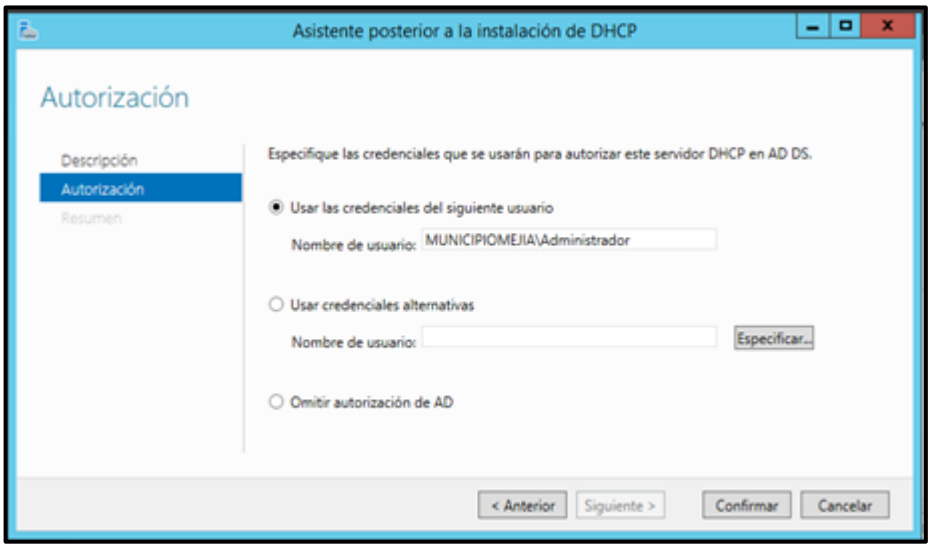
Figura 39. Descripción del servicio DHCP.



Fuente: Grupo investigador.

8. Nos aparece una nueva pantalla en la cual es el asistente para la instalación del DHCP, como lo observamos en la figura 40, nos aparece el nombre del usuario, si esta todo bien ponemos en la opción “Confirmar”.

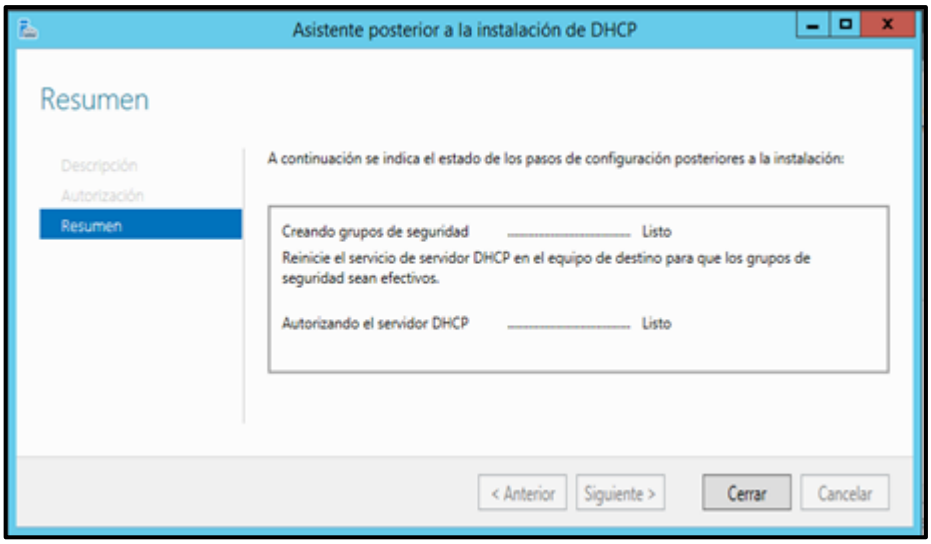
Figura 40. Asistente posterior para la instalación del servicio DHCP.



Fuente: Grupo investigador.

9. Una vez que se confirma, nos muestran una pantalla en lo cual nos muestra unos mensajes y debemos seleccionar el ítem “Cerrar”, como lo podemos observar en la figura 41, y ya está instalado nuestro servicio DHCP.

Figura 41. Estado de los pasos de configuración del servicio DHCP.

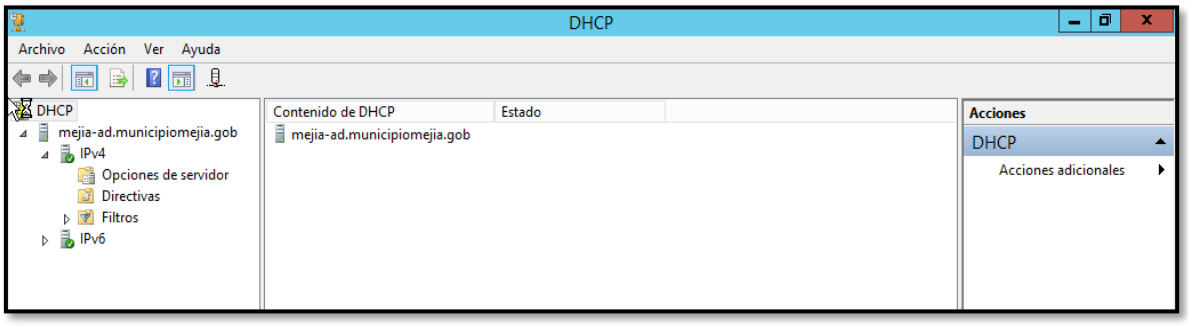


Fuente: Grupo investigador.

10.5.3.4. Configuración del servicio DHCP.

1. En la figura 42. Vamos a comenzar con la configuración del servicio DHCP, en lo cual vamos a herramientas del administrador del servidor, en la opción DHCP, y nos aparece una ventana nueva, en la cual seleccionamos DHCP y nos aparece en nombre del dominio junto al DHCP y dos opciones IPv4, y IPv6.

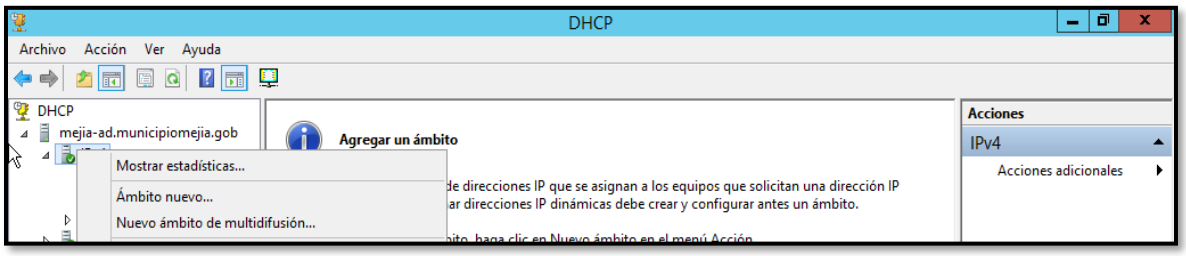
Figura 42. configuración del servicio DHCP.



Fuente: Grupo investigador.

2. En la figura 43, damos clic derecho en la opción IPv4, y seleccionar “Ámbito nuevo”.

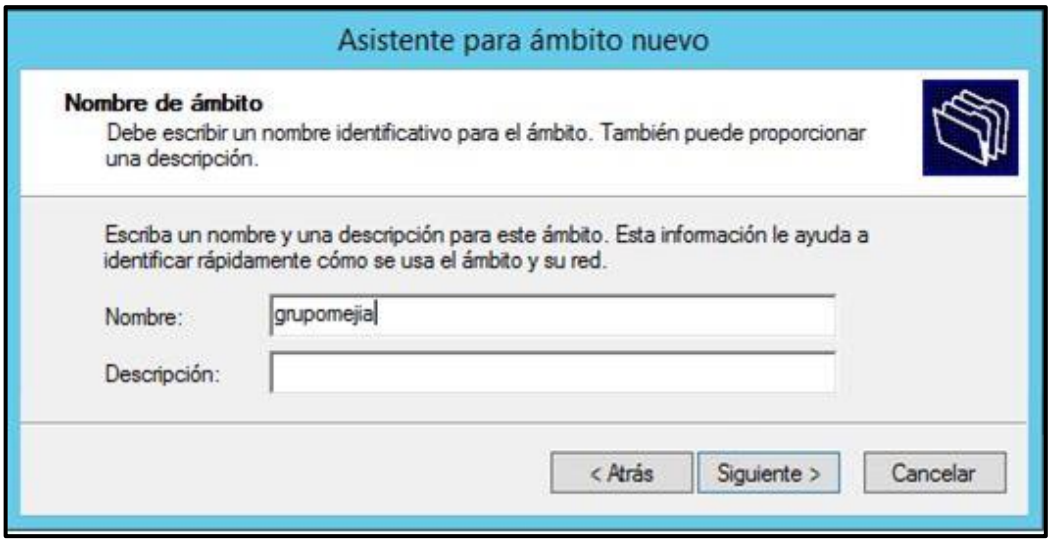
Figura 43. Creación de un Ámbito nuevo.



Fuente: Grupo investigador.

3. En la figura 44, nos aparece el asistente del ámbito nuevo en donde debemos dar clic en “Siguiente”, y nos aparece una nueva ventana en donde debemos crear un nombre del ámbito en este caso lo nombramos grupomejia.

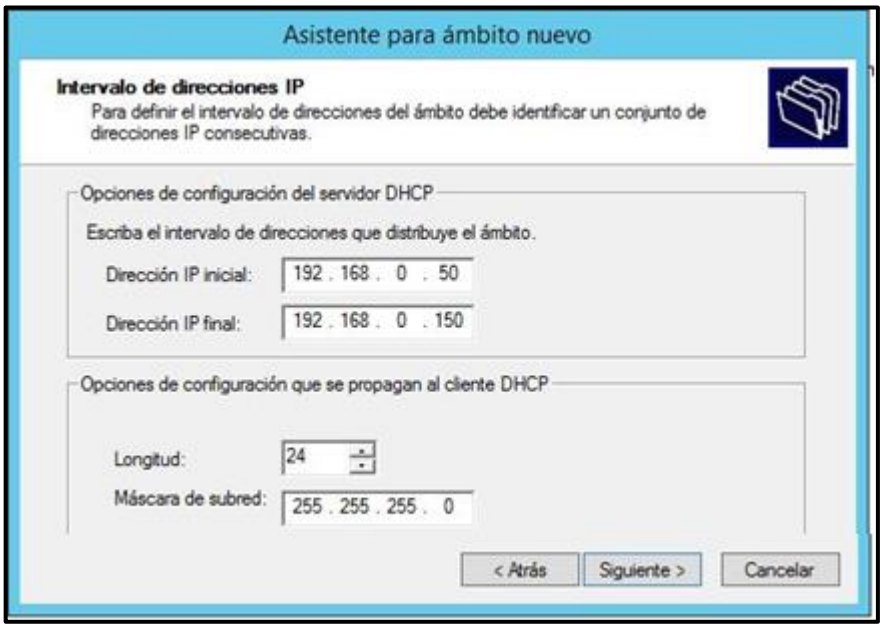
Figura 44. Nombre del ámbito.



Fuente: Grupo investigador.

4. Nos aparece la pantalla del Intervalo de direcciones IP en donde debemos poner las direcciones IP desde donde comienza y cuál sería el final, como podemos observar en la figura 45.

Figura 45. Intervalo de direcciones IP.



Fuente: Grupo investigador.

5. Al configurar las direcciones IP, nos aparece la pantalla de agregar exclusiones y retraso, esto nos permite excluir direcciones IP para la asignación de las impresoras u

otros artefactos tecnológicos, pero nosotros los dejamos vacío, porque no lo necesitamos como podemos observar en la figura 46.

Figura 46. Agregar exclusiones y retraso.

Fuente: Grupo investigador.

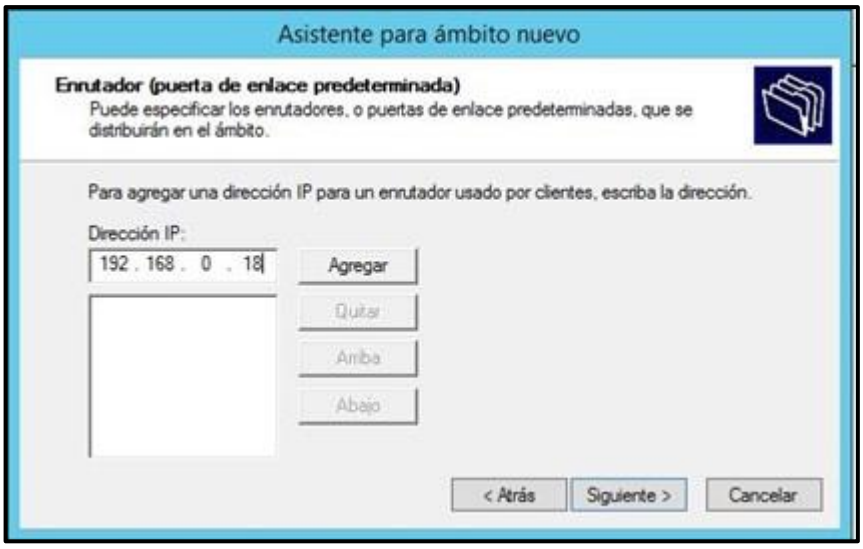
6. En la figura 47, podemos observar la pantalla de duración de la concesión, esto nos quiere decir que debemos ingresar cuantos días las maquinas van a permanecer con la dirección IP.

Figura 47. Dirección de la concesión

Fuente: Grupo investigador.

7. En la pantalla configuraciones opcionales del DHCP, solo damos clic en “Siguiente”, en la pantalla siguiente debemos agregar la dirección IP de enrutamiento que en este caso seria 192.168.0.18, como lo podemos observar en la figura 48.

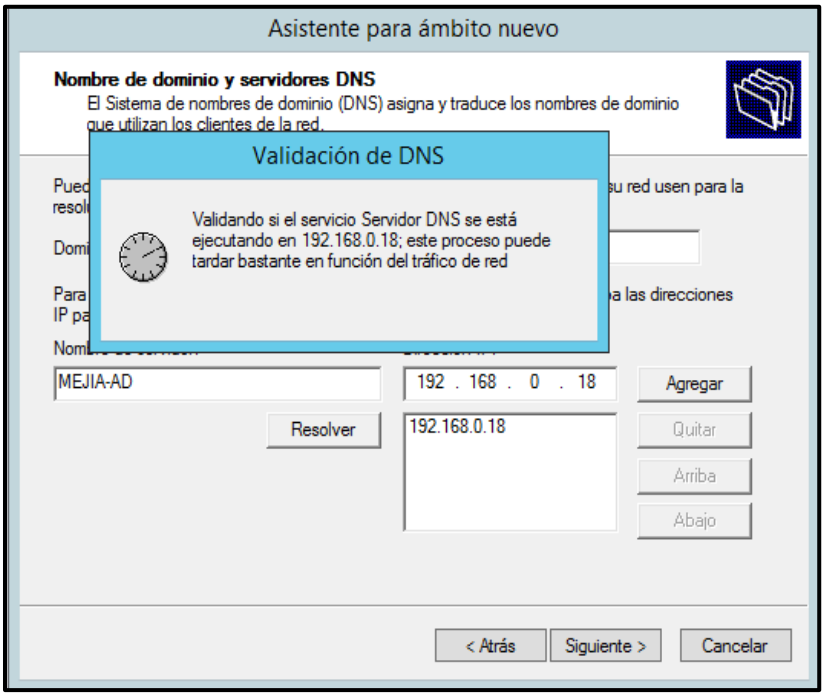
Figura 48. Enrutador (puerta de enlace predeterminado)



Fuente: Grupo investigador.

8. En la figura 49, Podemos observar que nos pide ingresar el nombre del servidor, una vez ingresado el servicio valida el DNS y si es el correcto aparecen las direcciones IP.

Figura 49. Validación de DNS.



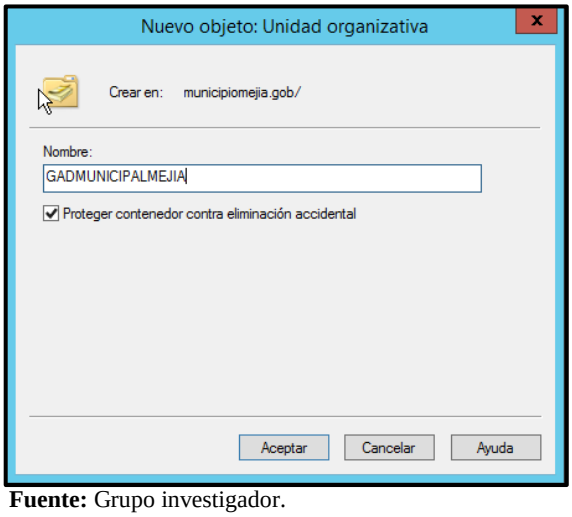
Fuente: Grupo investigador.

9. Una vez echo toda la configuración nos va a parecer la última pantalla que nos da un mensaje de Finalización del asistente para el ámbito nuevo, lo único que pulsamos es Finalizar y el proceso de configuración del servicio DHCP ha culminado.

10.5.3.5. Creación de usuarios y equipos en el Active Directory

- En la figura 50, vamos a crear las unidades organizativas del GAD Municipal del Cantón Mejía para eso nos vamos al Administrador de servidor – Herramientas – Usuarios y equipos del Active Directory, nos aparecerá el nombre del dominio, damos clic derecho y agregamos una nueva Unidad organizativa que en este caso tendría el nombre principal GADMUNICIPALMEJIA.

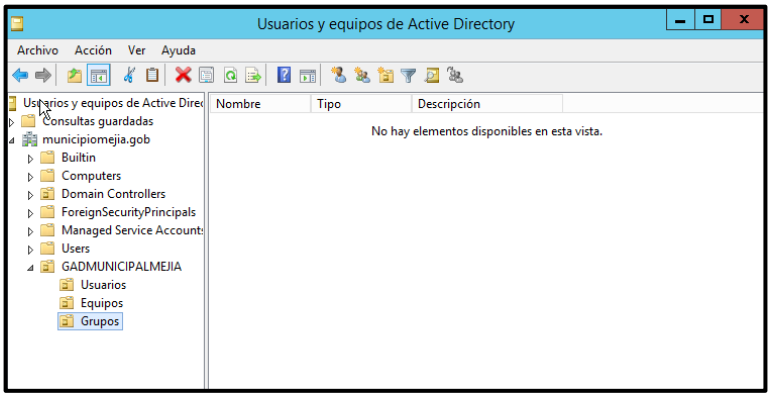
Figura 50. Creación de la Unidad Organizativa



Fuente: Grupo investigador.

- Después de crear la raíz vamos a crear las categorías que van dentro de la carpeta en la cual vamos a nombrar 3 las cuales son: Usuarios, Grupos y Equipo, como lo podemos observar en la figura 51.

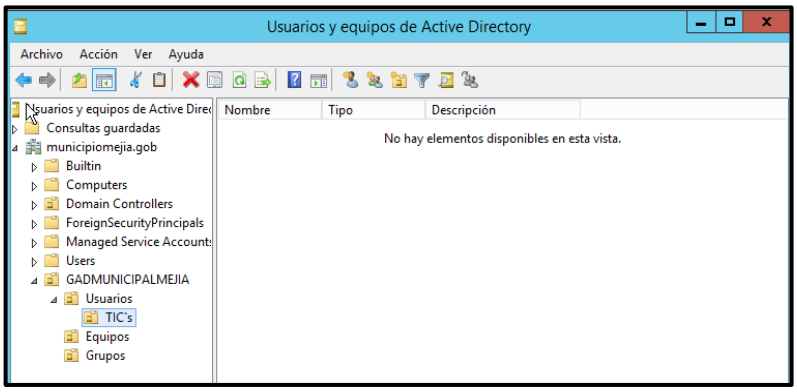
Figura 51. Ingreso de Categorías



Fuente: Grupo investigador.

- En la figura 52, vamos a especificar qué carpetas van en cada una de las categorías, como en la categoría Usuarios, vamos a enumerar cada una de los departamentos que posee en GAD Municipal, en Grupos se van a especificar los usuarios comunes, y en los Equipos se van a visualizar todos los equipos que están dentro del dominio.

Figura 52. Ingreso de Subcategorías



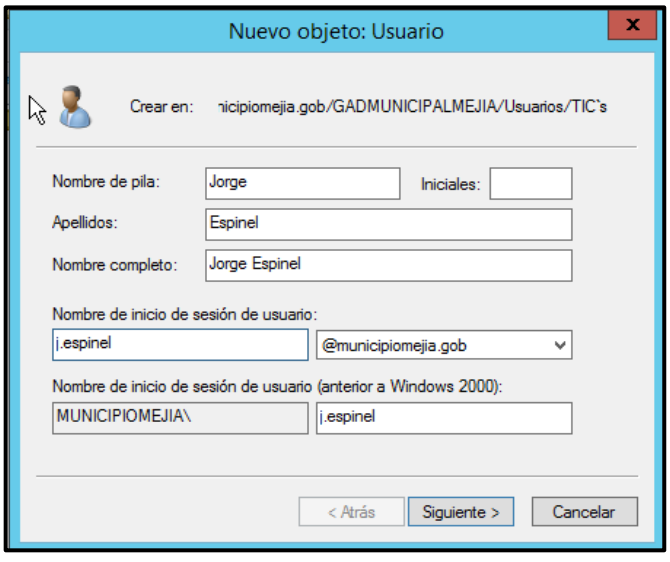
Fuente: Grupo investigador.

10.5.3.6. Creación de usuarios y contraseñas

Una vez creada todas las Unidades organizativas, vamos a crear los usuarios para unirlos con el dominio.

- En la figura 53. Vamos a la categoría de Usuarios, y damos clic derecho en un departamento que hayamos creado, ponemos nuevo usuario, en donde nos aparece que ingresemos, su nombre y su apellido y nos pide que ingresemos un nombre de inicio de sesión en donde por políticas del GAD vamos a ingresar la primera inicial del nombre. Apellido en este caso quedaría j.espinel.

Figura 53. Ingreso de inicio de sesión de usuario

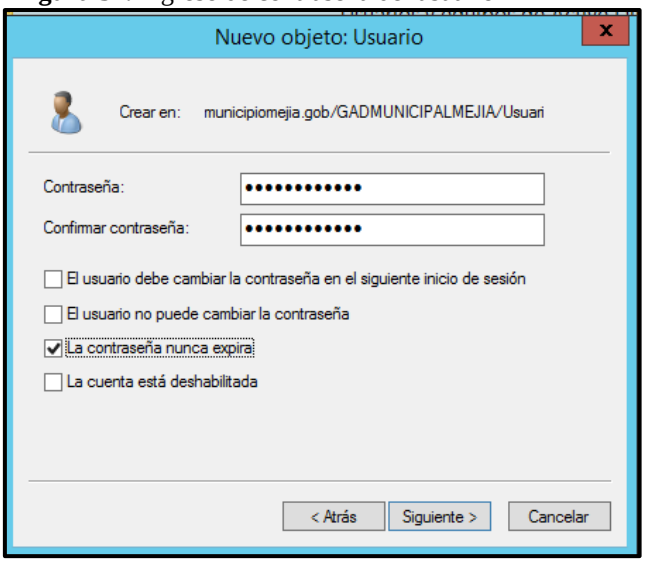


Fuente: Grupo investigador.

- Una vez creado el usuario vamos a la siguiente ventana el cual nos muestra que debemos ingresar una contraseña en donde vamos a ingresar su primer nombre con el año en el

que nos encontramos, vamos a marcar la opción de la contraseña nunca expire como lo podemos observar en la figura 54.

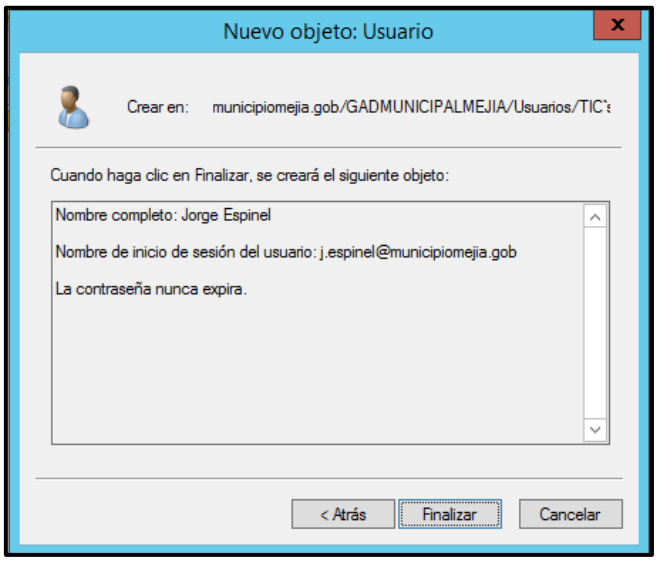
Figura 54. Ingreso de contraseña del usuario



Fuente: Grupo investigador.

- En la figura 55, vamos a ver las características del usuario que vamos a crear.

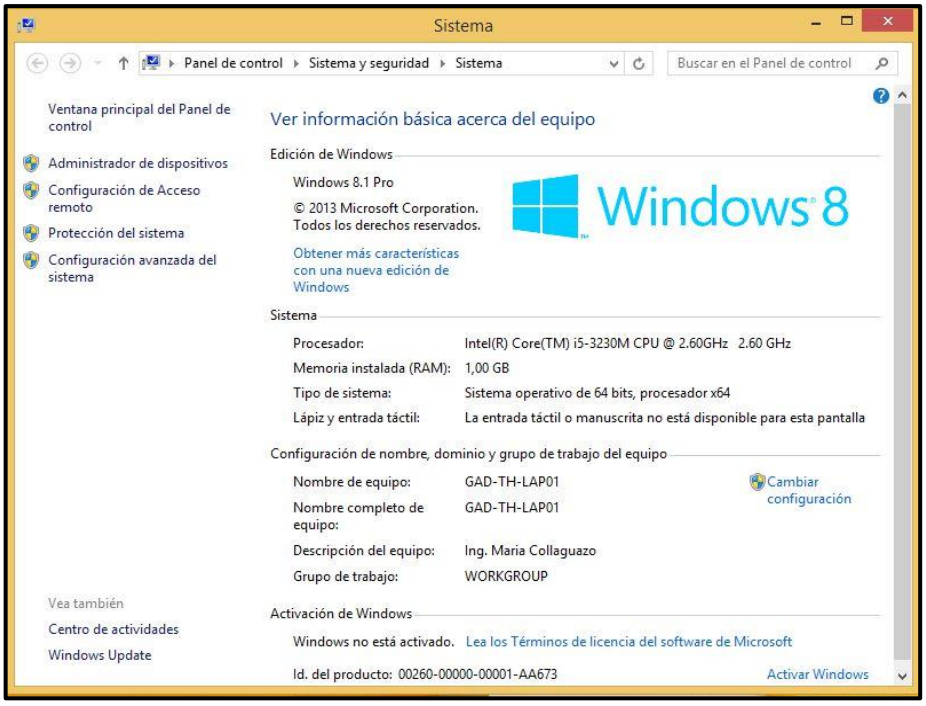
Figura 55. Características de la creación del usuario



Fuente: Grupo investigador.

- Una vez creado el usuario vamos a otro equipo en donde vamos a Mi Pc, Clic derecho y vamos a cambiar el nombre del equipo, como podemos observar en la figura 56, y vamos a poner una descripción en este caso el nombre del usuario que lo está utilizando.

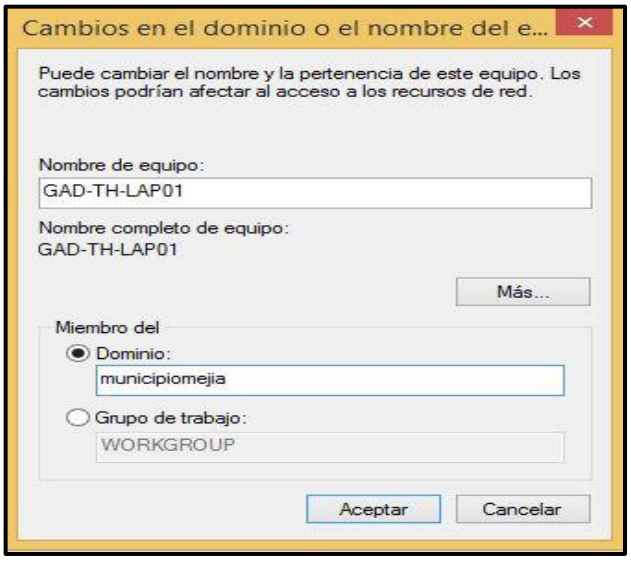
Figura 56. Cambio del nombre de equipo y añadir descripción



Fuente: Grupo investigador.

- Vamos a la opción cambiar configuración en donde nos aparecerá la pantalla cambios de dominio, vamos a la opción miembro de dominio y ahí introducimos el nombre de nuestro dominio que configuramos. Como vemos en la imagen 57.

Figura 57. Ingreso al dominio



Fuente: Grupo investigador.

Como podemos observar ya está creado los usuarios respectivos ahora debemos ver cuáles son los resultados después de hacer todas estas configuraciones.

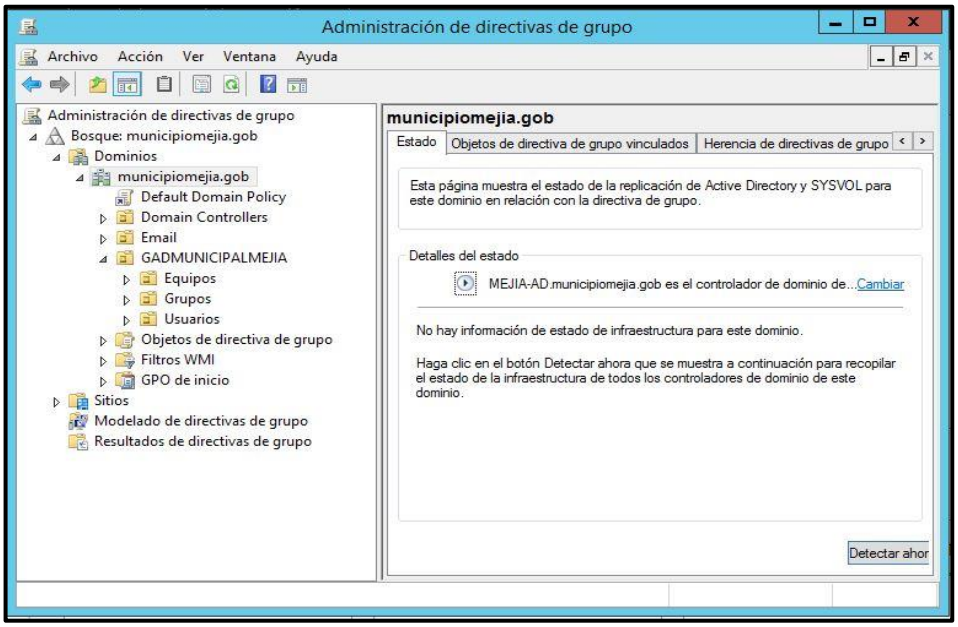
10.5.3.7. Creación de Políticas del Active Directory

Vamos a establecer las políticas del active directory ya que es un complemento que esta herramienta trae.

Fondo de pantalla.

- Nos dirigimos a la opción administración de directivas de grupo en donde nos aparece esta ventana como podemos ver en la figura 58.

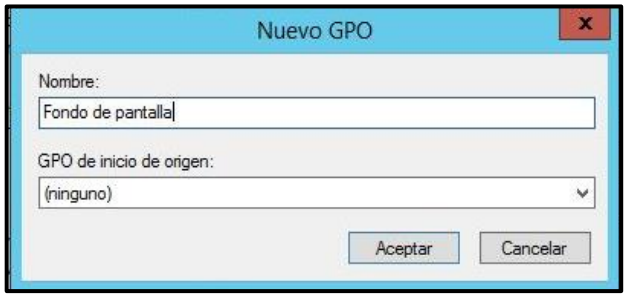
Figura 58. Ingreso a la administración de directivas de grupo



Fuente: Grupo investigador.

- En donde vamos a dar clic derecho en nuestro dominio, y podremos crear un nuevo GPO en la cual le vamos a nombrar Fondo de pantalla como lo vemos en la figura 59.

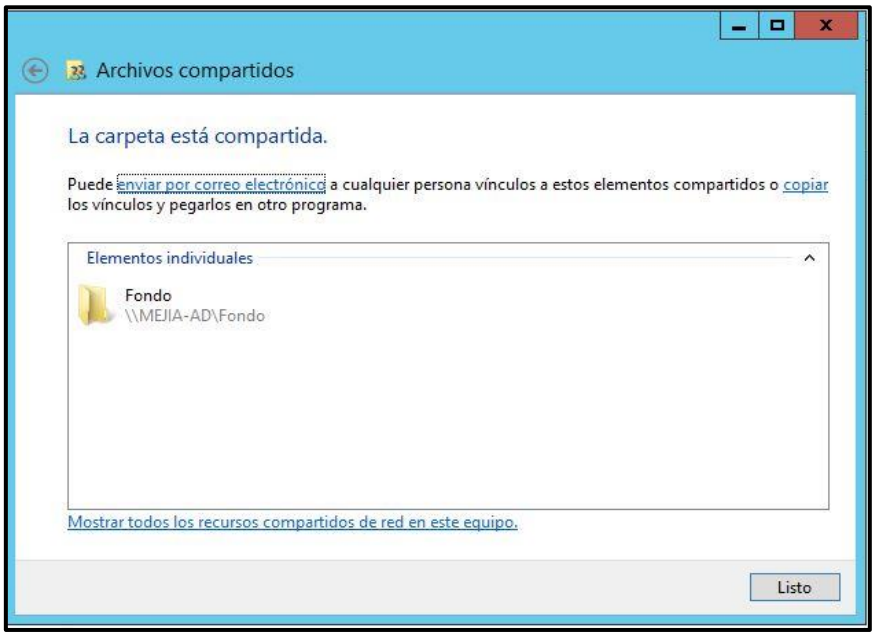
Figura 59. Nuevo GPO del fondo de pantalla



Fuente: Grupo investigador.

- Para crear este fondo de pantalla debemos ir al Disco C: y crear una carpeta compartida en donde vamos a guardar la imagen, como lo podemos observar en la figura 60.

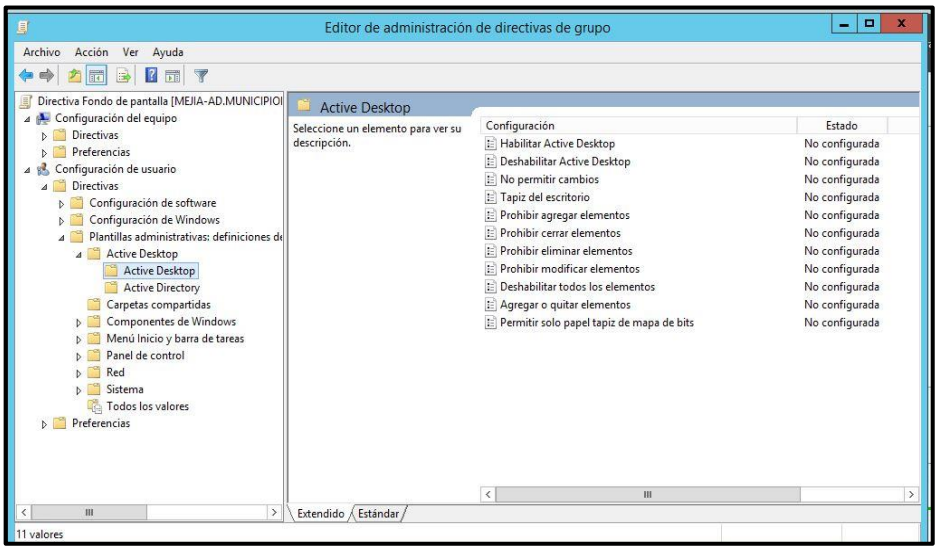
Figura 60. Carpeta compartida para el fondo de pantalla



Fuente: Grupo investigador.

- Una vez compartida la carpeta nos dirigimos de nuevo a la administración de directivas de grupo en donde el GPO creado vamos a dar clic derecho y editar, luego de eso vamos a las siguientes opciones: Configuración de usuario – Directivas – Pantillas administrativas definidas – Active Directory – Active Directory, como lo podemos ver en la figura 61.

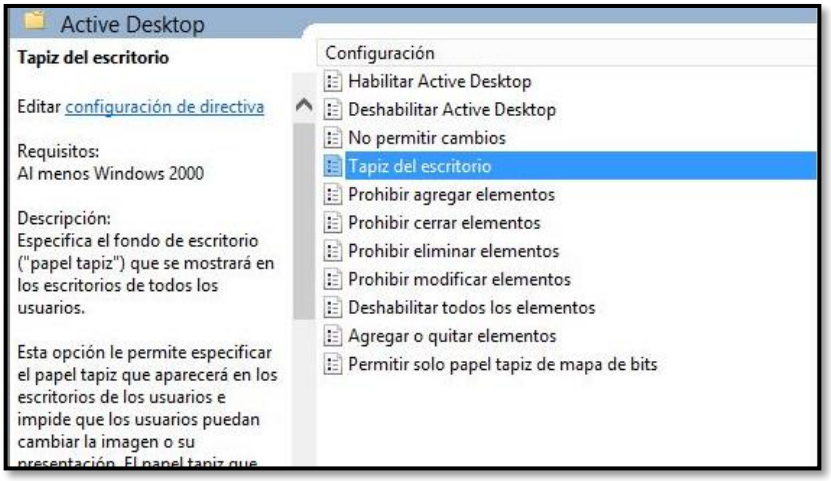
Figura 61. Proceso para ingresar política de fondo de pantalla



Fuente: Grupo investigador.

- Vamos a configurar 3 opciones la cual tenemos “Habilitar Active Desktop”,” No permitir cambios”,” Tapiz del escritorio”, como lo observamos en la figura 62.

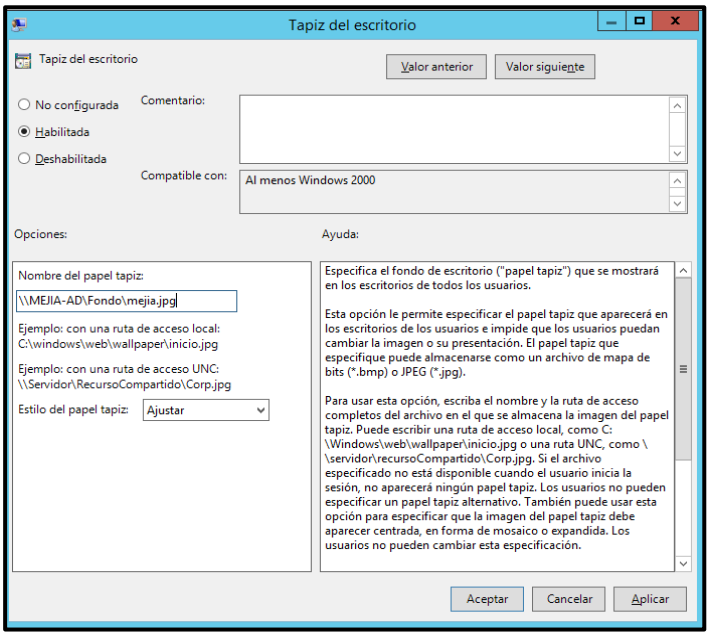
Figura 62. Configuración del fondo de pantalla



Fuente: Grupo investigador.

- En la figura 63, vamos a modificar el Tapiz del escritorio, para poder insertar el fondo de pantalla, damos clic en habilitar, vamos a la carpeta compartida que está ubicada en el disco C: de ahí le copiamos el nombre y lo colocamos dentro del nombre de papel tapiz, luego de eso vamos a ingresar el nombre de la imagen acompañado del JPG, que es la extensión de la imagen, en el estado del papel tapiz lo que vamos hacer es coger alguna opción para que se refleje el tamaño.

Figura 63. Configuración del Papel Tapiz



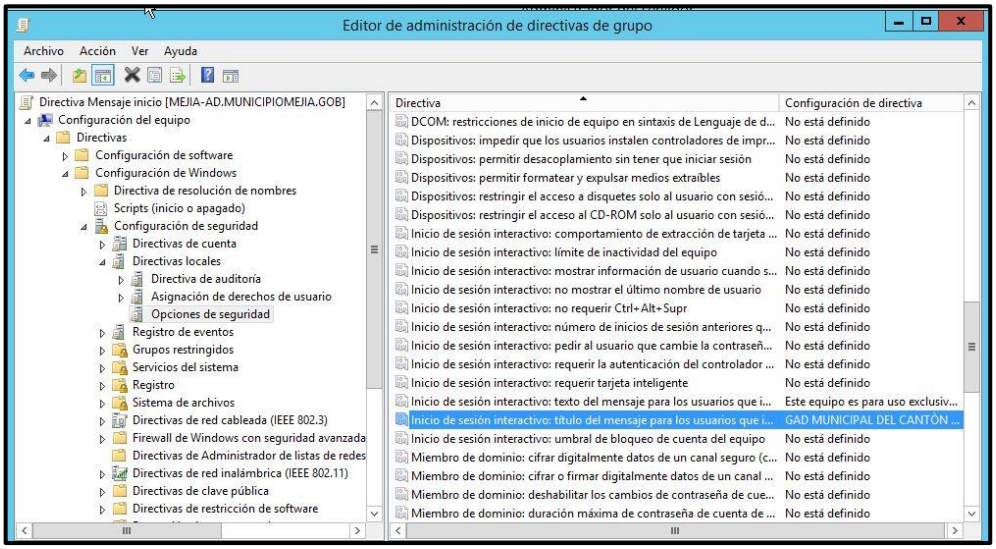
Fuente: Grupo investigador.

Mensaje de Inicio

- Debemos crear una GPO con el nombre de “Mensaje de Inicio”. En la figura 65, vamos a editar el GPO del mensaje nuevo vamos a la siguiente pestaña “Confirmación del

equipo", y luego – Configuración de Windows – Configuración de seguridad – Directivas locales y en las opciones de seguridad debemos configurar dos opciones "Inicio de sesión: texto del mensaje para los usuarios" y "Inicio de sesión: Título del mensaje para los usuarios".

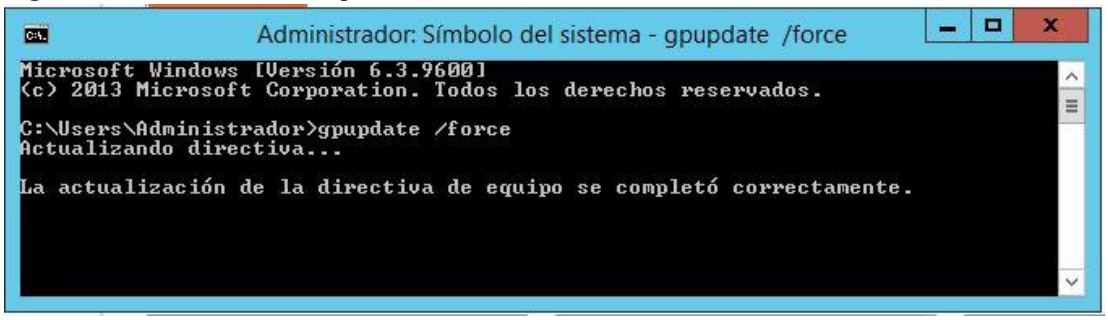
Figura 64. Configuración del GPO del mensaje de inicio



Fuente: Grupo investigador.

- Para que se puedan actualizar las políticas que hemos configurado debemos abrir el CMD, y escribimos la palabra gpupdate /force ese comando nos permite actualizar las políticas que hemos añadido. Como lo observamos en la figura 65.

Figura 65. Actualización de la política

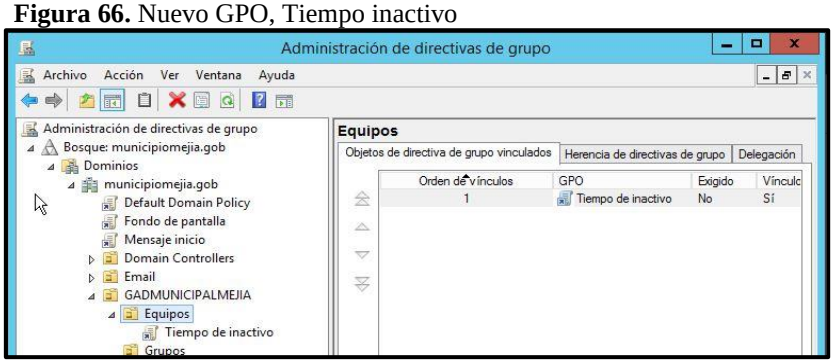


Fuente: Grupo investigador.

Tiempo inactivo

- Esta política se va a crear en la carpeta de Equipos que está dentro de la raíz del dominio, con el nombre Tiempo inactivo, como lo observamos en la figura 66.

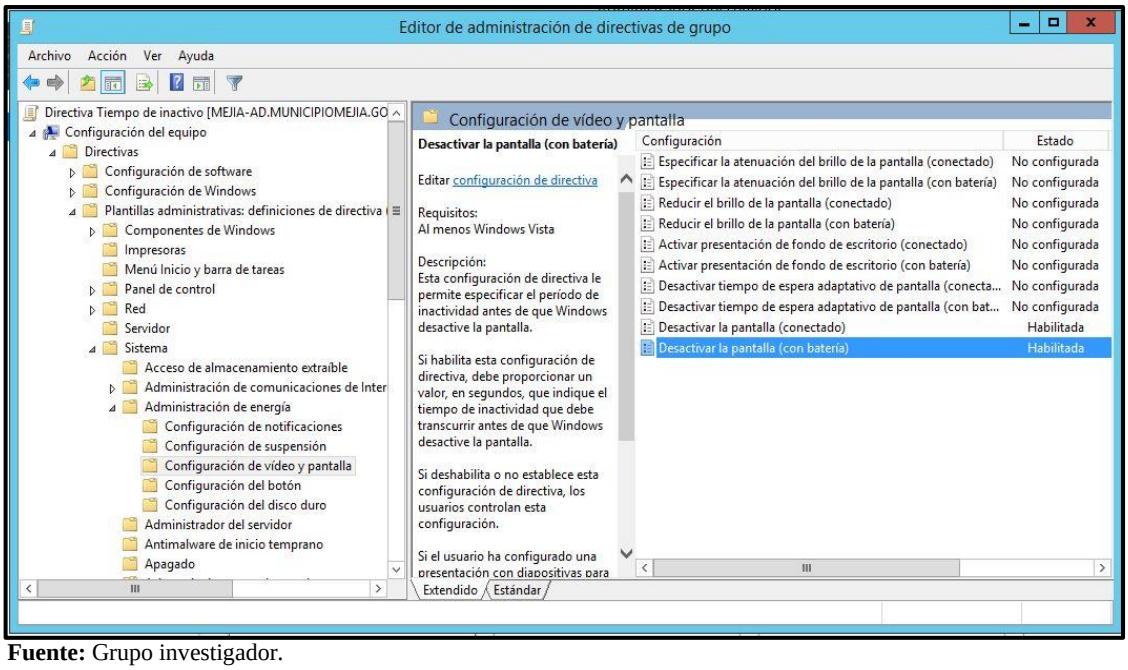
Figura 66. Nuevo GPO, Tiempo inactivo



Fuente: Grupo investigador.

- Una vez creada la política vamos a la opción editar ingresamos a la opción "Configuración del equipo", y damos clic en Directivas – Plantillas administrativas definiciones de directiva – Sistema – Administración de energía y configuración de video y modificamos las siguientes opciones: "Desactivar la pantalla (conectado)" y "Desactivar la pantalla (con batería)", como lo vemos en la figura 67.

Figura 67. Opciones de política tiempo inactivo

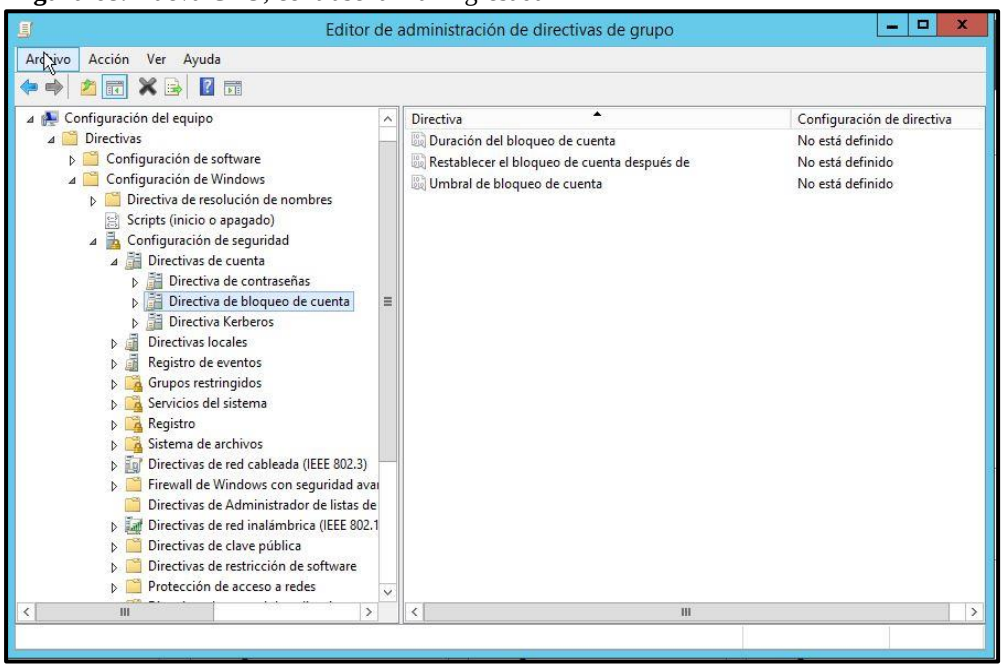


Fuente: Grupo investigador.

Contraseña mal ingresada

- Para proceder debemos crear una política que nos diga contraseña mal ingresada vamos a las siguientes configuraciones: al ítem: Configuración del equipo – Directivas – Configuración de Windows – Configuración de seguridad – Directivas de cuente – Directiva de bloqueo de cuenta, como observamos en la figura 68.

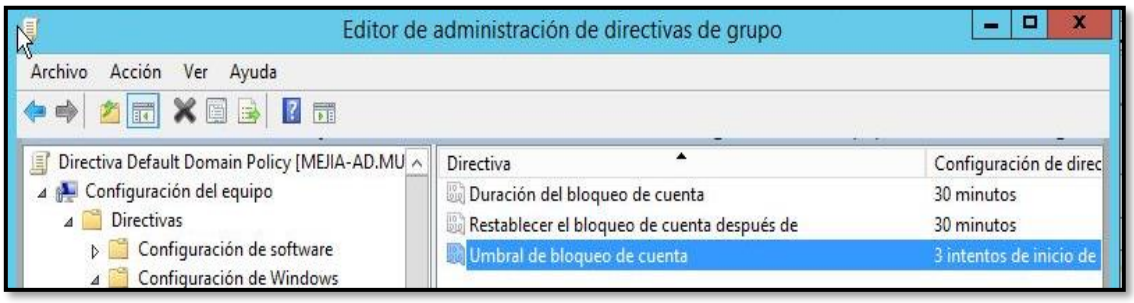
Figura 68. Nueva GPO, contraseña mal ingresada



Fuente: Grupo investigador.

En la figura 69 vamos a configura las siguientes opciones las cuales son: Duración del bloqueo de cuenta, Restablecer el bloqueo de cuenta después de y Umbral de bloqueo de cuenta

Figura 69. Configuración del GPO, Contraseña mal ingresada



Fuente: Grupo investigador.

10.5.3.8. Configuración de la Autenticación de Active Directory con Zimbra Collaboration.

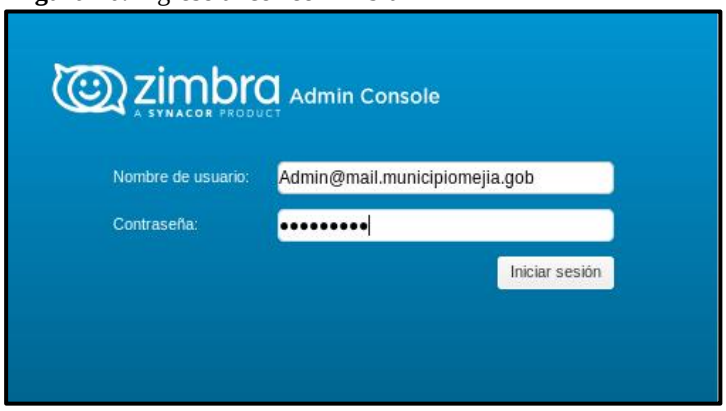
Cuando Active Directory se usa para administrar la autenticación de los usuarios dentro de la red, Zimbra Collaboration debe configurarse para mantener las contraseñas sincronizadas. La configuración se la realiza mediante consola de administración a través del navegador.

Para la Autenticación del Active Directory con Zimbra Collaboration vamos a empezar configurando en el Zimbra desde el Administrador.

1. Para configurar el modo de autenticación de Zimbra, accedemos a la consola de administración escribiendo desde el navegador la dirección https://192.168.0.10:7071.

Ingresamos el nombre de usuario y contraseña, luego hacemos clic en Iniciar sesión, tal como vemos en la figura 70.

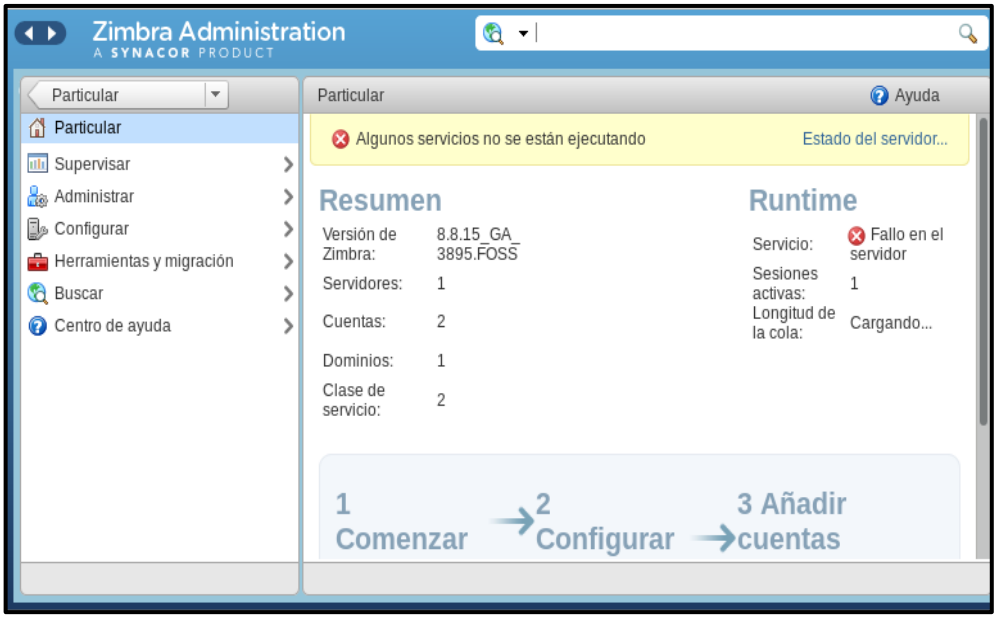
Figura 70. Ingreso al correo Zimbra



Fuente: Grupo investigador.

2. Seleccionamos la opción de: Configurar elemento en el lado izquierdo de la ventana, tal como se indica en la figura 71.

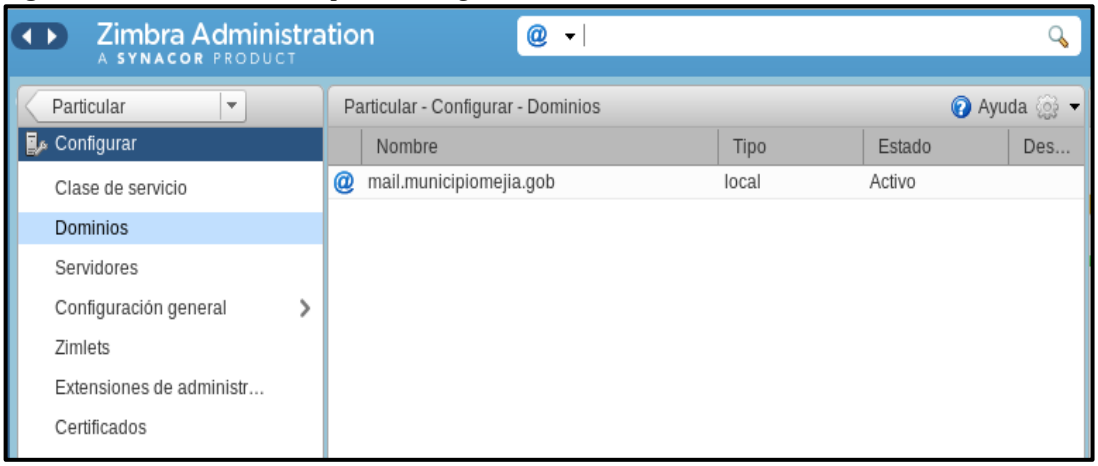
Figura 71. Selección de la opción Configurar



Fuente: Grupo investigador.

3. Luego hacemos clic en Dominios en el lado izquierdo, como se observa en la figura 72 y procedemos hacer clic con el botón derecho en el dominio para configurar y seleccionamos la opción Configurar autenticación.

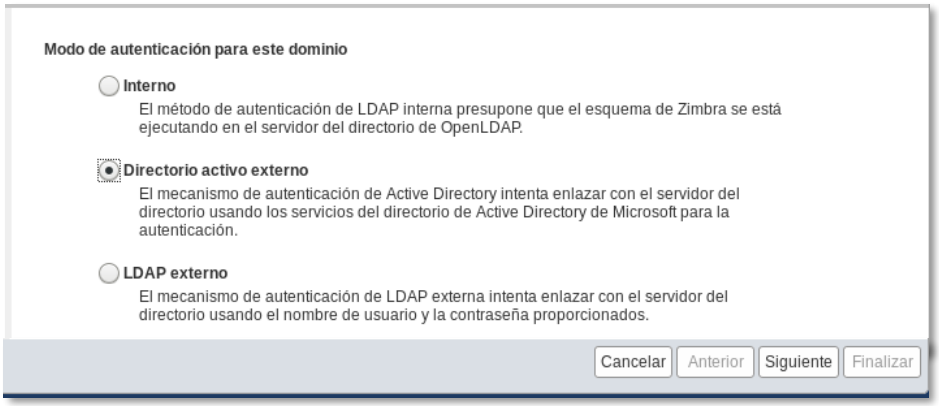
Figura 72. Seleccionamos la opción Configurar autenticación



Fuente: Grupo investigador.

4. Seleccionamos la opción de Directorio activo externo como se ve en la figura 73, y hacemos clic en siguiente.

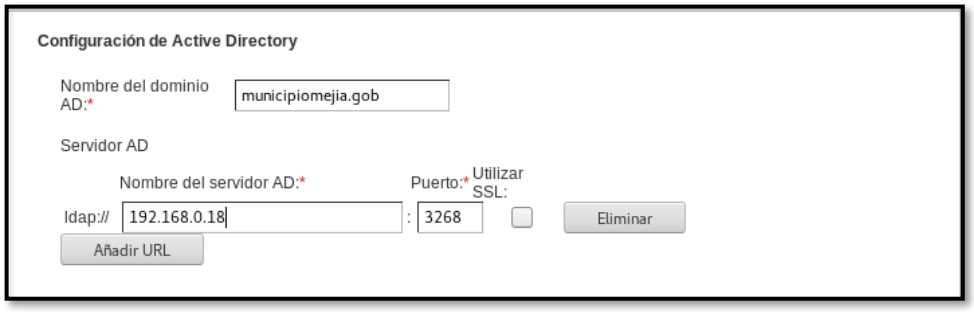
Figura 73. Selección del Directorio activo externo



Fuente: Grupo investigador.

5. Escribimos el nombre de dominio AD e insertamos la dirección IP del controlador de dominio que específica el Puerto LDAP, como se muestra en la figura 74, y hacemos clic en siguiente.

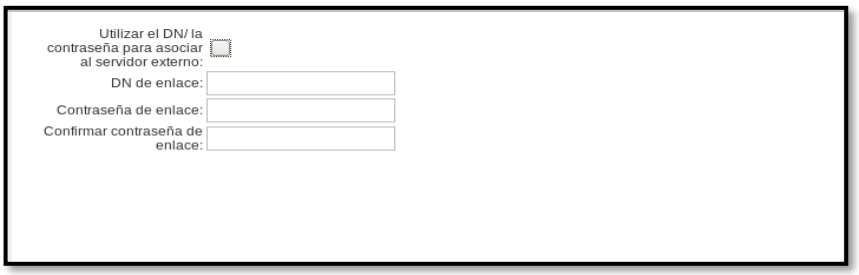
Figura 74. Ingresamos el Nombre del Dominio AD, nombre del servidor AD



Fuente: Grupo investigador.

6. Dejamos por defecto tal como se indica en la figura 75, Y damos en siguiente

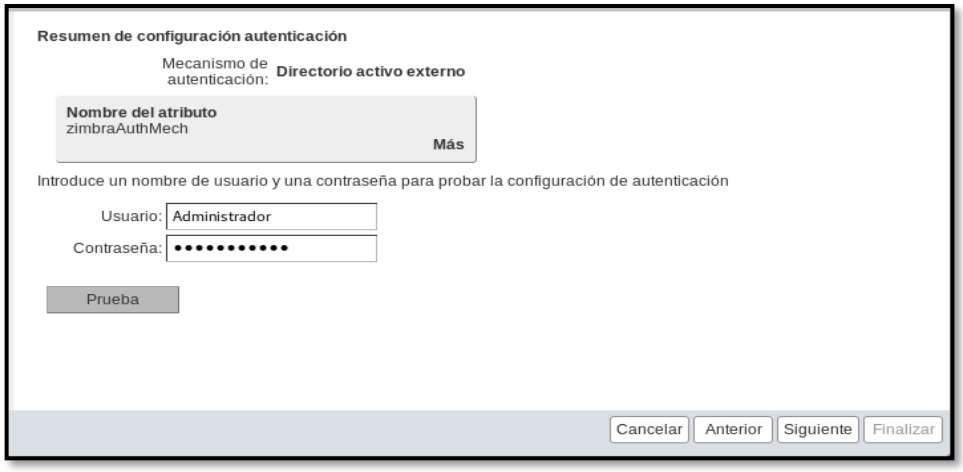
Figura 75. Proceso continuo a la configuración



Fuente: Grupo investigador.

7. Escribimos el nombre de usuario y la contraseña de la cuenta de Active Directory para autenticar tal como se muestra en la figura 76, y hacemos clic en el botón Prueba para verificar la cuenta.

Figura 76. Ingreso de Usuario y contraseña de la cuenta del Active Directory



Fuente: Grupo investigador.

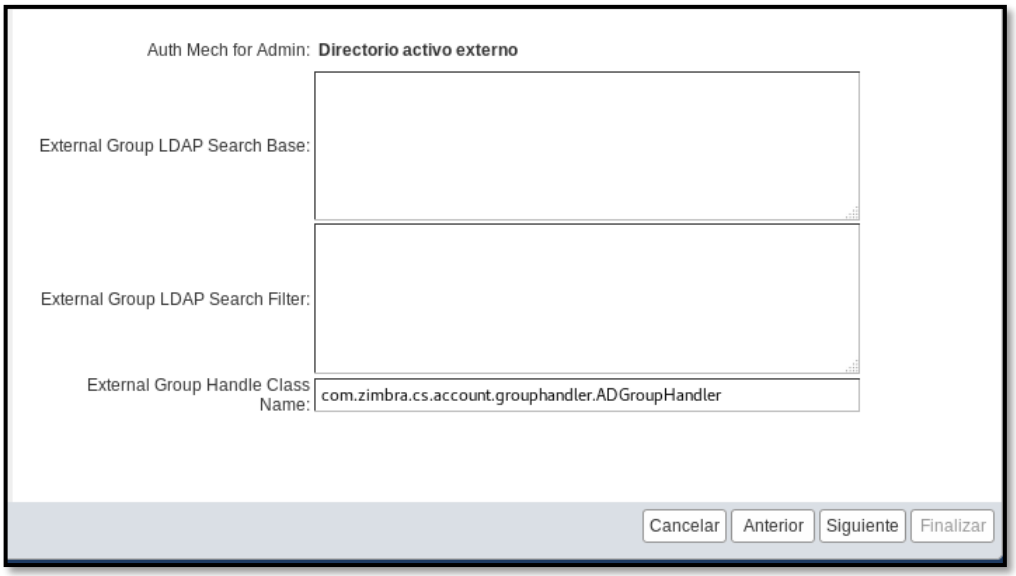
8. Si todo se ha configurado correctamente, la cuenta se autentica sin problema alguno como se observa en la figura 77, verificamos la conectividad y damos clic en siguiente.

Figura 77. Prueba de autenticación

Fuente: Grupo investigador.

9. Dejamos el valor predeterminado y luego le damos en la opción siguiente, se puede apreciar en la figura 78.

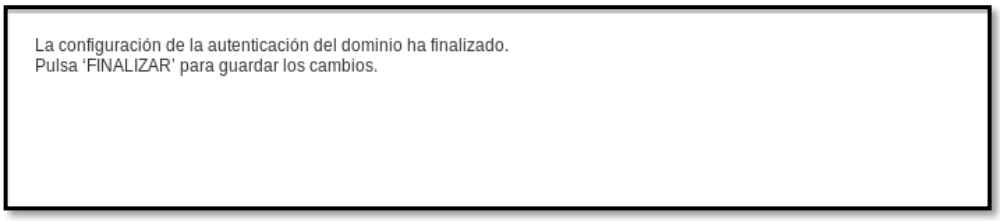
Figura 78. Valor predeterminado



Fuente: Grupo investigador.

10. Como se puede observar en la figura 79, la configuración está completa y hacemos clic en Finalizar para guardar los cambios.

Figura 79. Autenticación de dominio finalizado



Fuente: Grupo investigador.

11. ANÁLISIS Y DISCUSIÓN DE LOS RESULTADOS.

11.1. Análisis técnico operativo

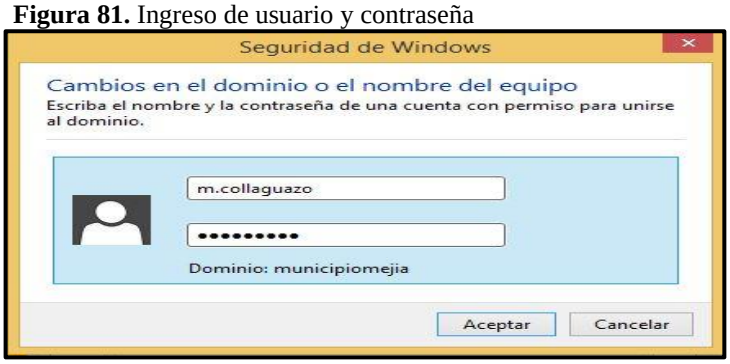
11.1.1. Prueba de conexión del usuario correcto

Como resultados vamos a poder observar que luego de poner el nombre del dominio como podemos observar en la Figura 80, directamente se no abre otra pantalla, como se ve en la figura 81, en cual debemos ingresar el usuario y la contraseña que fue creada en el servidor, como lo vemos en las figuras.

Figura 80. Ingreso del nombre del dominio

Fuente: Grupo investigador.

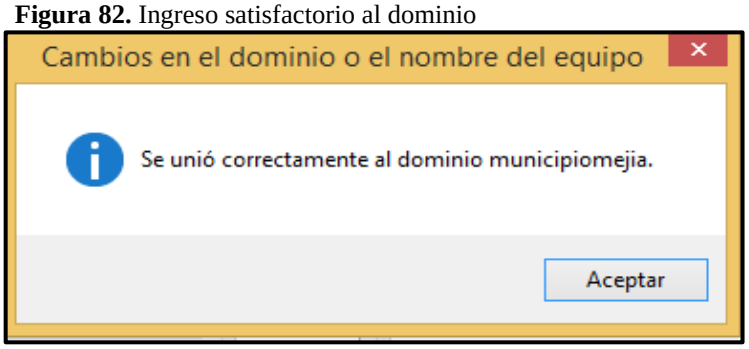
Figura 81. Ingreso de usuario y contraseña



Fuente: Grupo investigador.

Podemos observar que después de este ingreso de usuario y contraseña nos sale un mensaje se unió al dominio correctamente, como vemos en la figura 82 nos pide que le reiniciemos al ordenador.

Figura 82. Ingreso satisfactorio al dominio



Fuente: Grupo investigador.

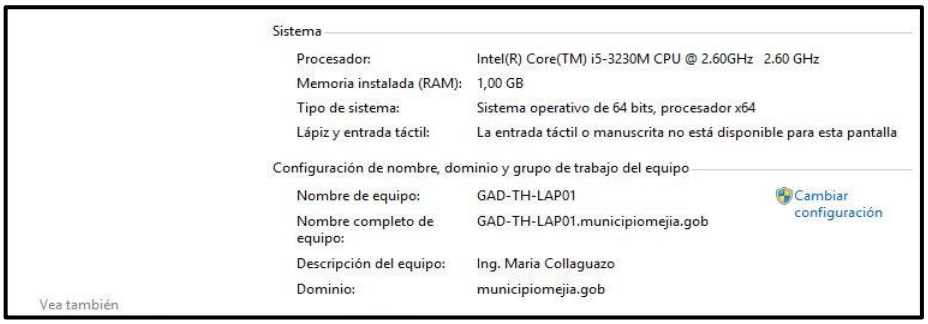
Al momento que el equipo se reinicia nos aparece nosotros ponemos otro usuario, he ingresamos el usuario y contraseña, pero debemos ver el nombre del dominio que correspondo al municipiomejia.gob, como se observa en la figura 83.

Figura 83. Ingresar el usuario y la contraseña en el equipo

Fuente: Grupo investigador.

Una vez que ingresemos los datos se va a abrir en Windows 8, para comprobar que estamos en el dominio vamos a MI PC, y propiedades y vamos a ver como aparece el nombre de nuestro equipo junto con el nombre del dominio, como lo podemos observar en la figura 84.

Figura 84. Verificación de ingreso al dominio



Fuente: Grupo investigador.

Debemos tener en cuenta que para unirle al dominio siempre debemos estar conectados a la misma red y ahí no nos va a causar ningún tipo de problemas.

11.1.2. Políticas de seguridad

En la Figura 85. Cuando nosotros prendemos a la maquina nos aparece un mensaje informativo, debemos poner aceptar y continuar ingresando la contraseña del Usuario que tenga.

Figura 85. Política de mensaje de inicio

Fuente: Grupo investigador.

Como resultado de esta política vamos a ver que al momento de encender el computador nos aparece un mensaje, mostrando a que entidad pertenece el dominio y un mensaje de aviso para los usuarios que están en la entidad, la cual el botón “Aceptar” nos ayuda para pasar a la siguiente ventana que es para ingresar el usuario y contraseña.

Política de fondo de pantalla

En la figura 86. Vamos a poder observar que los equipos que tienen en el GAD Municipal del Cantón Mejía trabajan con Windows 8, en donde le con ayuda a la política que posee Windows Server 2012, pudimos modificar el fondo de pantalla donde nos muestra el logo de la entidad, para que esta política se actualice debemos ingresar al CMD y escribir gpupdate /force para que se actualice las políticas, vamos al equipo del usuario y le reiniciamos para que pueda actualizar los cambios.

Figura 86. Política de Fondo de pantalla

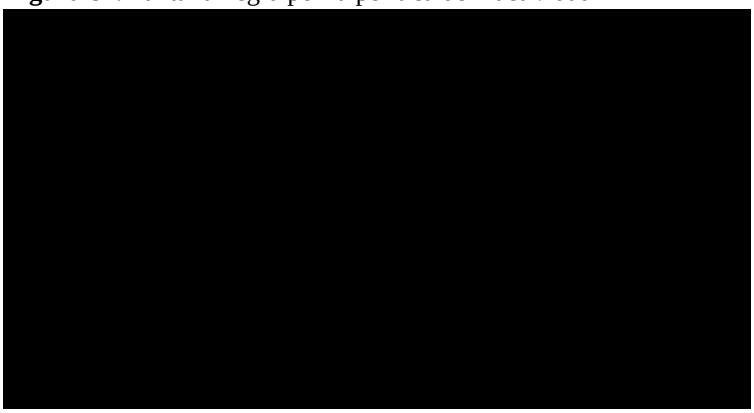
Fuente: Grupo investigador.

Debemos tener en cuenta que para insertar esta política debemos elegir una imagen legible y de buen tamaño para que la imagen no se dañe al momento de añadirlo.

Política tiempo inactivo

En la figura 87, podemos observar la política de inactividad en la cual consiste en el tiempo que no se ocupa el computador se bloquea mostrándonos una pantalla negra de fondo, nosotros pulsamos las teclas CTRL + ALT + SUPR, para poder ingresar la contraseña como lo vemos en la figura 88, y volver a ingresar al computador y seguir trabajando.

Figura 87. Pantalla negra por la política de inactividad



Fuente: Grupo investigador.

Figura 88. Ingreso de contraseña

Fuente: Grupo investigador.

Política de contraseña mal ingresada

En la figura 89 vamos a observar que al momento de ingresar una clave errónea 3 veces nos va a salir un mensaje como esto “La cuenta a que se hace referencia está bloqueada y no se puede utilizar”.

Figura 89. Política de mal ingresado la contraseña

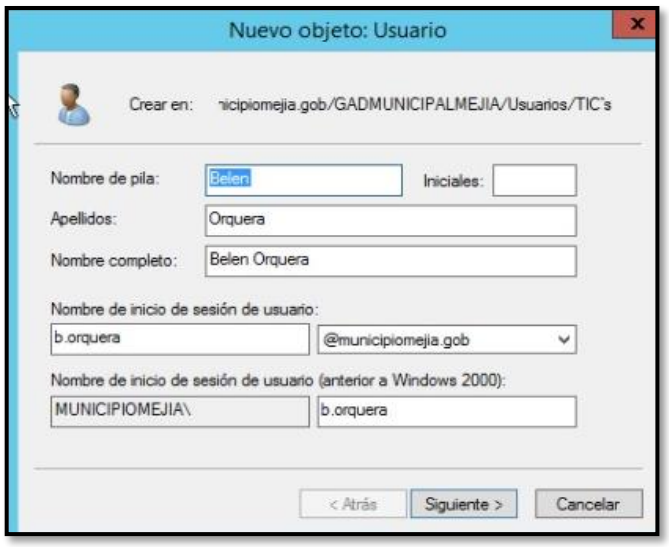
Fuente: Grupo investigador.

Una vez bloqueada la cuenta debemos ir al servidor de dominio de dar clic en propiedades del usuario para poder desbloquearlo.

11.1.3. Creación de una cuenta en el Active Directory

Como se puede apreciar en la figura 90, se realiza la creación de un nuevo usuario, llenando todos los campos solicitados.

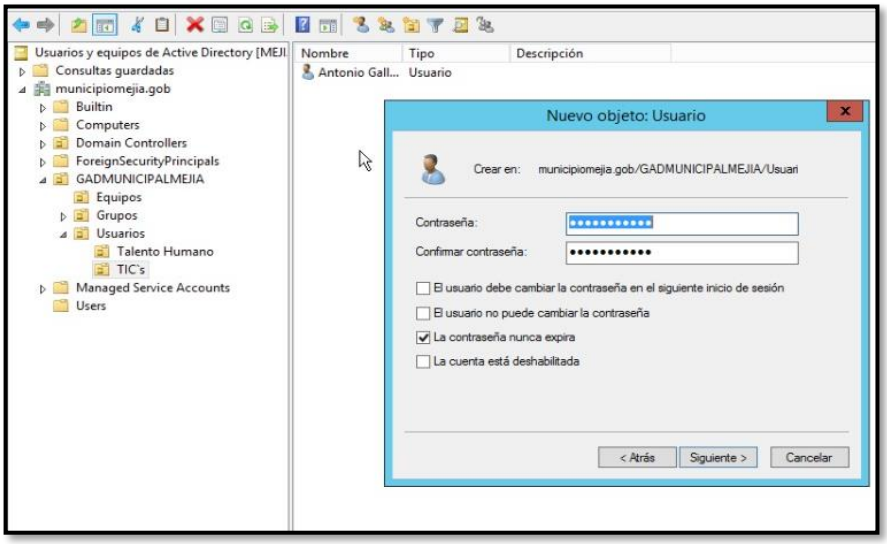
Figura 90. Creación de un nuevo usuario



Fuente: Grupo investigador.

Se procede a crear la contraseña del usuario, tal como se ve en la figura 91, la cual será utilizada más adelante.

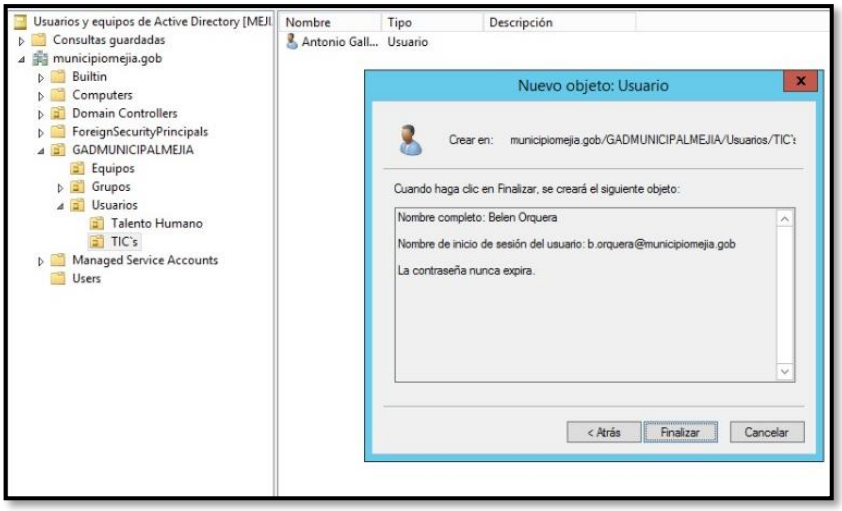
Figura 91. Creación de la contraseña del usuario



Fuente: Grupo investigador.

Una vez realizado el proceso de creación de usuario, le damos en la opción Finalizar, esto se puede apreciar en la figura 92.

Figura 92. Usuario creado en el Active Directory

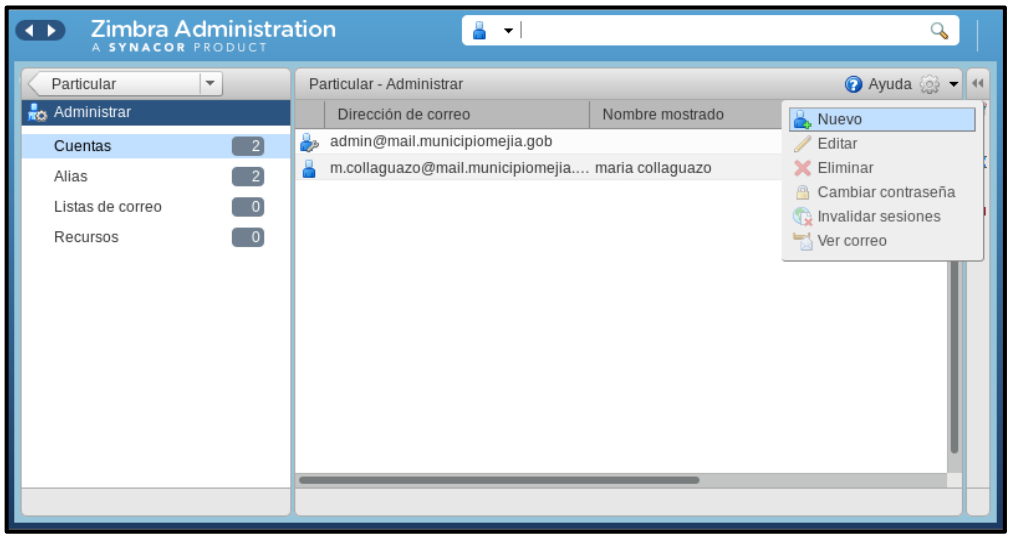


Fuente: Grupo investigador.

11.1.4. Sincronización de Zimbra con Active Directory

Para sincronizar Zimbra Collaboration con Active Directory, se ha creado con el mismo nombre de cuenta en el sistema Zimbra. Desde la consola de administración, para esto se ha seleccionado Administrar y en la opción Nuevo crear una nueva cuenta, todo esto se puede apreciar en la figura 93.

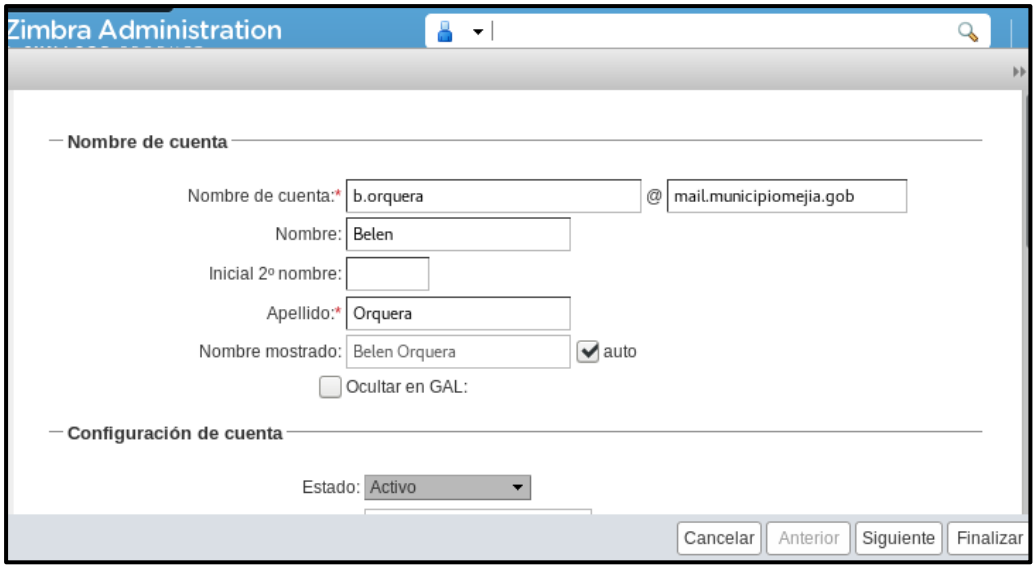
Figura 93. Creación de la cuenta nueva en Zimbra



Fuente: Grupo investigador.

Se escribe el mismo nombre de cuenta establecido en el Active Directory y el dominio utilizado, tal como se puede observar en la figura 94.

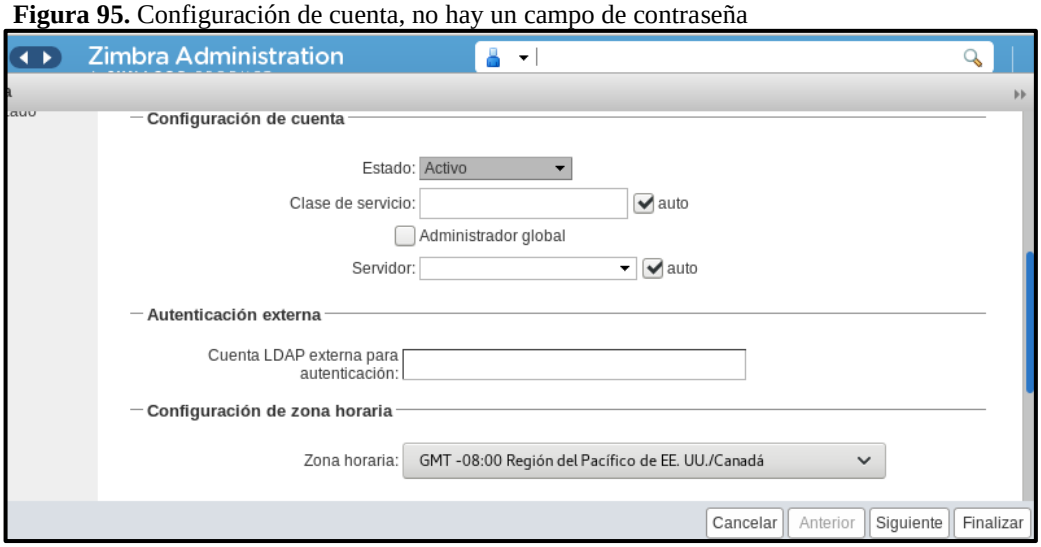
Figura 94. Ingreso de los mismos datos del Active Directory en Zimbra



Fuente: Grupo investigador.

Como se puede ver en la figura 95, no hay un campo de contraseña presente en las opciones de Nueva cuenta. Esto se debe a que la contraseña se toma directamente del Active Directory. Hacemos clic en Finalizar para crear la cuenta.

Figura 95. Configuración de cuenta, no hay un campo de contraseña



Fuente: Grupo investigador.

Prueba de Autenticación

Abrimos el navegador y accedemos al correo de Zimbra tal como se puede ver en la figura 96, escribiendo el IP_Address del servidor o el nombre público de DNS (es decir, mail.municipiomejia.gob). Cuando aparezca la pantalla de autenticación de Zimbra, escribimos el nombre de usuario y la contraseña de la cuenta que acaba de crear y luego hacemos clic en el botón Iniciar sesión.

Figura 96. Ingreso del usuario y contraseña en Zimbra

Fuente: Grupo investigador.

Tal como se ve en la figura 97, la autenticación se realizó correctamente, por lo que se abre la página de correo web del usuario de Zimbra. La cuenta utilizada se ha autenticado directamente desde Active Directory.

Zimbra ahora está configurado correctamente para autenticar usuarios con Active Directory.

Figura 97. Cuenta autenticada directamente desde el Active Directory

Fuente: Grupo investigador.

11.1.5. Validación de la Hipótesis

Forma Teórica

Una vez realizado el correspondiente proyecto de investigación, y a ver seguido los distintos procesos para dar solución a la hipótesis planteada al inicio, se pudo llegar a la conclusión de que el servidor de dominio para el GAD Municipal del cantón Mejía, ha sido factible y aceptada en su gran mayoría por parte del Jefe del Departamento de Tics, dando un resultado positivo y de esta manera comprobando que el servidor de dominio ayuda a garantizar el acceso a recursos y servicios, y así los usuarios tienen un mejor acceso a la red, de esta manera se pudo corroborar que la investigación fue cumplida y terminada.

12. IMPACTOS (TÉCNICOS, SOCIALES, AMBIENTALES O ECONÓMICOS)

12.1. Técnico

El presente proyecto de investigación genera un gran impacto a nivel técnico, porque se realizó la creación de un servidor de dominio mediante un administrador de cuentas de seguridad, lo cual consiste en la autenticación y autorización en toda la red del GAD Municipal de Cantón Mejía, para lo cual se utilizó Windows Server 2012, agregando características de alta disponibilidad y centralizando los servicios en sí.

12.2. Social

A nivel social también se ha generado un impacto positivo, debido a que las personas que trabajan en el municipio disponen de servicio de comunicaciones actualizadas que les brindan la mejor experiencia de usuario y así también se puede decir que facilita el desarrollo de sus labores diarias. Generando de esta manera comodidad, satisfacción y sobre todo seguridad al utilizar los servicios tecnológicos de comunicaciones.

12.3. Económico

Con respecto al tema económico y ha obtenido de igual manera un impacto positivo, ya que el proyecto realizado para el GAD Municipal del Cantón Mejía, es de gran importancia y a su vez se ha logrado mayor seguridad con las cuentas de los usuarios, sin utilizar un costoso presupuesto para el municipio, se ha visto las formas más cómodas eficientes y seguras para el desarrollo del ismo dentro del municipio.

13. PRESUPUESTO PARA LA PROPUESTA DEL PROYECTO

13.1. Gastos Directos

Tabla 9. Descripción de Gastos Directos.

Recursos	Detalle	Cantidad	V. Unitario	V. Total
Materiales y suministros	Impresiones	50	0,05	15,00
	Copias	50	0,03	3,60
	Resmas de papel Bond	1	3,00	3,00
	Esferos	5	0,35	1,75
	Cuadernos	2	1,50	3,00
Equipos	Laptop´s	2	650,00	1.300,00

	Router	1	26,00	26,00
Servicios Básicos	Internet	5 meses (10 MG)	22,40	112,00
	Transporte	87 días	5,00	435,00
	Alimentación	87 días	3,00	261,00
Entregables	Anillados del proyecto	6	7,00	42,00
	Empastados	2	15,00	30,00
TOTAL				**2.232,35**

Fuente: Grupo investigador.

13.2. Gastos Indirectos

Tabla 10. Descripción de los gastos indirectos.

Fuente: Grupo investigador.

13.3. Gastos Aproximados

Tabla 11. Descripción de los gastos aproximados

Descripción	**Total**
Gastos Directos	$2.232,35
Gastos Indirectos	$2.092,48
Imprevistos + 10%	$432.48
Total, de Gastos	**$4.324,83**

Fuente: Grupo investigador.

14. CONCLUSIONES Y RECOMENDACIONES

14.1. Conclusiones

- Una vez analizado los diferentes contextos del administrador de cuentas de seguridad, el directorio activo y los protocolos, se logró comprender el significado de cada uno de estos y el papel que cumplen en el control de la información, para mantener las cuentas de los usuarios y equipos protegidos, y existe una mejor organización de la red en todo el municipio, brindando de esta forma estabilidad y el control oportuno de los equipos.

- Mediante la investigación de campo realizada en el GAD Municipal del Cantón Mejía, en el departamento de TIC´s se pudo obtener información clara del cómo se encontraba la infraestructura y el funcionamiento de los equipos y servidores, dando como resultado un panorama de inestabilidad con las cuentas de los usuarios y equipos, ya que no existía el control adecuado de la información y por ende tampoco se tenía la seguridad correspondiente.

- Con la realización del servidor de dominio se lograron resultados positivos para todo el Municipio, la seguridad y estabilidad al centralizar los recursos de los equipos, ayudo a que exista una mejor forma de trabajar dentro del departamento de TIC´s, y de esta manera tener un mejor control de la red, garantizando así la creación segura de las cuentas de usuarios y el uso adecuado de parte del mismo.

- Con la administración del dominio, se logró centralizar los principales recursos, es decir los usuarios y la información, además se centralizo las actividades de configuración de los equipos, y las configuraciones importantes de seguridad. Con esto se mejoraron los procesos de administración tanto en tiempo como en forma, de tal manera que ahora solo el administrador es el que realiza las configuraciones en el equipo servidor y las distribuye a los equipos de la red del municipio. Este objetivo representa para los usuarios, contar con su información protegida y a salvo de modificaciones por usuarios que no sean dueños de la cuenta, dado el uso de credenciales de inicio de sesión que ahora se requiere en todos los equipos y por ende todos los usuarios.

14.2. Recomendaciones

- Para un buen rendimiento del Servidor de dominio, se recomienda hacer el uso del mismo con todos los servicios que mantenga el municipio, para que de esta manera exista un mejor desenvolvimiento del servidor y ayude en el ámbito laboral.
- Para una mejora estructuración de las políticas de seguridad del active directory, se recomienda se realice el análisis respectivo, conjuntamente con el Director Administrativo y el personal del departamento de TIC´s, ya que se debe analizar minuciosamente las diferentes políticas aplicadas.
- Se recomienda realizar la capacitación correspondiente al administrador encargado de manejar el servidor de dominio, para que pueda hacer uso del mismo sin problemas y tenga claro del cómo funciona.
- Se recomienda tener un servidor con más capacidad de memoria, ya que el municipio abarca más de 600 usuarios y el servidor actual que mantiene el GAD no es lo suficiente grande en memoria para tanto personal y esto puede provocar un problema a futuro.

15. BIBLIOGRAFÍA

Abreu, J. (Diciembre de 2014). *El Método de la Investigación.* Obtenido de Conscience: http://www.spentamexico.org/v9-n3/A17.9(3)195-204.pdf

Aguilar, M. (2013). *Ptolomeo.unam.* Obtenido de Dominio para la Administración centralizada de recursos de cómputo: http://www.ptolomeo.unam.mx:8080/xmlui/bitstream/handle/132.248.52.100/4368/Tesis.pdf?sequence=1

Armijos, J., & Candelario, E. (2018). *"Análisis de vulnerabilidad en los servicios Active Directory, DNS y DHCP instalados en los sistemas operativos Windows Server (2008, 2012, 2016) Utilizando herramientas de Test de intrusión".* Guayaquil: Universidad de Guayaquil.

Asuad, N. (Agosto de 2014). *Marco Lógico de la investigación científica.* Obtenido de http://www.economia.unam.mx/cedrus/descargas/Metodo%20Cientifico.pdf

Beltrán, S. (2019). Explotación avanzada del directorio activo. *u.catolica.edu.co*, 1-18.

Bonnet, N. (2013). Las bases imprescindibles para administrar y configurar su servidor. En *Windows Server 2012* (pág. 794). Ediciones ENI.

Bonnet, N. (2014). *Windows Server 2012 R2. Las bases imprescindibles para administrar y configurar su servidor.* Barcelona: Ediciones ENI.

Bonnet, N. (2018). *Windows Server 2016, Instalación, gestión del almacenamiento y computación.* Barcelona: Ediciones ENI.

Calzada, R. (2014). *Introducción al Servicio de Directorio.* Red académica y de investigación nacional.

Castillo, J. (5 de Enero de 2019). *LDAP: Qué es y para qué se utiliza este protocolo.*

Cerdán, J. (2014). *Administración de Sistemas Corporativos basados en Windows 2012, Server; Protocolos de red.* España: Universidad Politécnica de Valencia.

Cruz, D., Pacheco, R., & Vanegas, A. (2014). Guia de configuración y administración de servicios de red bajo Windows Server 2008. (Tesis de Ingeniería). *unanleon.edu.ni*, 6-13.

De la Cruz. (2018). *Zimbra.*

De la Cruz, J. (14 de 02 de 2014). *Zimbra: Integración con Active Directory.* Obtenido de https://www.jorgedelacruz.es/2014/02/10/zimbra-integracion-con-active-directory/

De la cruz, J. (22 de Enero de 2020). Obtenido de De la Cruz.es: https://www.jorgedelacruz.es/2020/01/22/zimbra-actualizar-a-zimbra-collaboration-8-8-15-patch-6-mejoras-bugs-resueltos-y-update-de-openssl/

Días, G., Armendáriz, I., Ruiz, E., & Castro, M. (2014). *Procesos y herramientas para la seguridad de redes.* Madrid: Universidad Nacional de Educación a Distancia.

García, D., López, G., & Benavides, R. (01 de Diciembre de 2014). *Universidad Nacional de Ingenieria Facultad de electronica y computacion*. Obtenido de https://ribuni.uni.edu.ni/1259/1/60074.pdf

García, M., Garrido, J. L., Gómez, D., & Romero, A. (04 de 12 de 2015). *CentOS.* Obtenido de CentOS: https://mirror.jkanetwork.com/Documents/University%20works/Investigaci%C3%B3n%20CentOS.pdf

González, C. (03 de Julio de 2015). *Análisis de vulnerabilidades del DNS.* Obtenido de core.ac.uk: https://core.ac.uk/download/pdf/148676586.pdf

Gordillo, K. (2014). *Diseño y configuración de una arquitectura de alta disponibilidad para el servicio de clúester de base de datos Microsoft SQL Server 2008R2, orientadas a empresas mediana con productos microsoft (Tesis e Ingeniería).* Guayaquil: Universidad de Guayaquil.

Gualotuña, D. (28 de Julio de 2016). *Repositorio UTC.* Obtenido de Migración de infraestructura de servicios Microsoft (Active Directory) de Windows server 2008 R2, hacia Windows server 2012 R2, utilizando la metodología MSF, para mejorar los servicios tecnológicos de la empresa COBISCORP, (Tesis de Ingeniería): http://repositorio.utc.edu.ec/bitstream/27000/3689/1/T-UTC-000039.pdf

Guijarro, A., Orozco, F., Molina, M., & Trejo, J. (2018). Guía de infraestructura tecnológica con Windows Server 2012, Un enfoque Empresarial. *COMPAS*, 189 - 201.

Hernández, Y., Martínes, M., & Martín, E. (2016). FREE ACTIVE DIRECTORY MANAGER (FRADMANAGER). *Ciencias*, 40-53.

IBM. (2014). *Redes Sistema de nombres de dominio (DNS).* Obtenido de https://www.ibm.com/support/knowledgecenter/es/ssw_ibm_i_72/rzakk/rzakkpdf.pdf

Iperius. (17 de Junio de 2019). *Active Directory: construcción y buenas prácticas.* Obtenido de https://www.iperiusbackup.net/es/active-directory-construccion-y-buenas-practicas/

Jimenéz, P., & Orellana, I. (2012). *DESARROLLO DE UNA APLICACIÓN PARA LA ENCRIPTACIÓN Y DESENCRIPTACIÓN DE LA INFORMACIÓN DE UN DIRECTORIO MEDIANTE AUTENTICACIÓN POR PKI UTILIZANDO TECNOLOGÍA ACTIVE DIRECTORY. (Tesis de Ingeniería).* Cuenca: Universidad del Azuay.

León Lafebré, M. E., Mota Orrala, E. A., & Navarrete Zambrano, J. M. (2011). *Implementación de un sistema de gestión de seguridad de la información usando la norma SO27000 sobre un sitio de comercio electrónico para una nueva institución bancaria aplicando los dominios de control ISO 27001:2005.* Quito: Universidad Litoral.

Lopez, F. (5 de Junio de 2013). *Montaje Servidor Windows Server 2008 R2 y Active Directory.* Obtenido de http://hdl.handle.net/10785/1543

Matthews, M. (2013). *WINDOWS SERVER 2008 GUÍA DEL ADMINISTRADOR.* México: McGRAW-HILL.

Maya, E. (2014). *Métodos y Técnicas de investigación.* México: Universidad Nacional Autónoma de México.

Melilla, C. (2010). *Manual de Zimbra.* Obtenido de https://s3.amazonaws.com/files.zimbra.com/public/collateral/Zimbra%20Collaboration%20Product%20Overview-ES.pdf

Microsoft. (2016). *Guia de comparación de características, técnicas de Windows Server 2016.* Obtenido de http://www.microsoft.com/WindowsServer2016

Microsoft. (19 de Abril de 2017). *Auditar SAM.* Obtenido de https://docs.microsoft.com/es-es/windows/security/threat-protection/auditing/audit-sam

Microsoft. (2017). *Windows Server 2016.* Obtenido de https://www.tecnozero.com/wp-content/uploads/2017/01/windows-server-2016-versiones.pdf

Microsoft, A. (2015). Obtenido de http://www.microsoft.com/es-es/server-cloud/products/windows-server-2012-r2/Features.aspx

Mungabusi, L. (2016). *Implementacion de una distribucion GNU/LINUX LSBS para la autenticacion de los usuarios y la seguridad de los recursos de red de la cooperativa de ahorro y credito escencia indigena Ltda.* Ambato: Universidad Técnica de Ambato.

Ocampo, L., & Vivanco, H. (17 de Julio de 2015). "Implementación de Active Directory aplicando el estándar 802.1x, dentro de la red LAN y WLAN de la Universidad Nacional de Loja". (Tesis de Ingeniería). Loja: Universidad Nacional de Loja.

Oleas, D. (2013). *"ANÁLISIS DE LAS IMPLEMENTACIONES DEL PROTOCOLO LDAP. CASO PRÁCTICO: IMPLATACIÓN DE UN SISTEMA DE AUTENTICACIÓN APLICADO A LOS LABORATOTIOS DE LA EIS" (Tesis de Ingeniería).* Riobamba: Escuela Superior Politécnica de Chimborazo.

Ortiz, F. (2015). *Informática.* Obtenido de Microsoft TechNet: https://slideplayer.es/slide/159972/2/images/5/Controlador+de+dominio.jpg

Pulido, M. (2015). *Ceremonial y protocolo: métodos y técnicas de investigación científica.* Venezuela: Universidad del Zulia.

Rodríguez, M. (2013). *Acerca de la Investigación Bibliográfica y Documental.*

Romero, C. (2018). *"Análisis comparativo entre productos que proveen servicios de directorio pertenecientes a Tecnologías propietaria y de libre acceso, aplicando a laboratorio en ambientes educativos" (Tesis de Ingeniería).* Guayaquil: Escuela Superior Politécnica del Litoral.

Ruiz, M. (2013). *EL ENFOQUE MIXTO DE INVESTIGACIÓN EN LOS ESTUDIOS FISCALES.* España : Revista Académica de Investigación.

Ruiz, P. (15 de Agosto de 2013). *Active Directory*. Obtenido de SomeBooks: http://somebooks.es/3-2-conceptos-basicos-en-una-estructura-de-directorio-activo/

Sierra, F. (10 de Diciembre de 2014). *Directivas del Grupo (GPO) en Windows Server 2012.* Obtenido de https://cetatech.ceta-ciemat.es/2014/12/directivas-de-grupo-gpo-en-windows-server-2012/

Solanes, J. (5 de Septiembre de 2016). *MSolanes.* Obtenido de Introducción a Active Directory: https://www.jmsolanes.net/es/introduccion-active-directory/

Vanjones, M., Deman, T., Elmaleh, F., & Ddesfarges, G. (2018). *WINDOWS SERVER 2016, Administración avanzada.* Barcelona: Ediciones Software (ENI).

Yosimar Olvera, O., & Rizo Gaona, J. C. (2013). *Imlementacion de un dominio en el centro de apoyo a la docencia del CELE para la optimizacion de sus recursos y servicios. (Tesis de Ingeniería).* México: Universidad Nacional Autónoma de México.

16. ANEXOS

16.1. Anexo 1: Hoja de vida del Grupo de trabajo

DATOS PERSONALES

Nombres: Alex Christian

Apellidos: Llano Casa

Fecha de nacimiento: 09 de noviembre de 1986

Edad: 34 Años

Estado civil: Casado

Ciudad de domicilio: Tanicuchi

Dirección: Barrio Cajon Veracruz

Teléfono celular: 0999969302

E-mail institucional: alex.llano9864@utc.edu.ec

DATOS ACADÉMICOS

Tercer Nivel "Ingeniero en Informática y Sistemas Computacionales"

Maestría o Equivalente "Master Universitario en Ingeniería de Software y Sistemas Informáticos"

CURSOS Y CERTIFICADOS

Curso Internacional en Cultura de la Investigación

Desarrollo de Competencias Docentes 2da Edición

Metodologías de la Investigación y Proyectos

EXPERIENCIA LABORAL

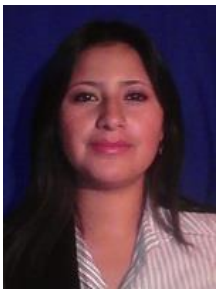
Ministerio de Telecomunicaciones y de la Sociedad de la Información

Aglomerados Cotopaxi Sa

Empresa Durini Industria De Madera Ca

Compuventas y Servicios Latacunga

AUTORAS:



Nombres: María Belén

Apellidos: Collaguazo Quinatoa

Fecha de Nacimiento: 20/06/1995

Edad: 24 años

Estado Civil: Soltero

Ciudad de domicilio: Quito

Dirección: Barrio las Casas sector Obispo Díaz de la Madrid

Teléfono Celular: 0987067114

Cédula: 050396047-8

Correo institucional: maria.collaguazo8@utc.edu.ec

ESTUDIOS PRIMARIOS:

Escuela Fiscal Mixta "Macas"

Latacunga-Ecuador

ESTUDIOS SECUNDARIOS

Colegio Técnico "Sara María Bustillos de Atiaga"

Latacunga-Ecuador

ESTUDIOS SUPERIORES

Universidad Técnica de Cotopaxi

Actualmente cursando Décimo semestre de Ingeniería en Informática y Sistemas Computacionales.

Latacunga – Ecuador

AUTORAS:

Nombres: Diana Nataly

Apellidos: Toapanta Chilig

Fecha de nacimiento: 18 de abril del 1994

Edad: 25 Años

Estado Civil: Soltera

Ciudad de domicilio: Tambillo

Dirección: Barrio la Merced, calle principal.

Teléfono Celular: 0979194370

E-mail institucional: diana.toapanta6@utc.edu.ec

ESTUDIOS PRIMARIOS:

Escuela Fiscal Mixta “Isabel Yánez”

Machachi – Ecuador

ESTUDIOS SECUNDARIOS

Unidad Educativa “Nueva Primavera”

Quito – Ecuador

ESTUDIOS SUPERIORES

Universidad Técnica de Cotopaxi

Actualmente cursando Décimo semestre de Ingeniería en Informática y Sistemas Computacionales.

Latacunga – Ecuador

16.2. Anexo 2: Política al encender el equipo

	POLÍTICA AL ENCENDER EL EQUIPO	PO-1E
		Ver No. 01
		Pág.1 de 2

1. Objetivo

Definir e implementar lineamientos del encendido de equipo con respecto a la información que se presente al momento de que el usuario haga uso del mismo, mediante la recopilación de información en el departamento de tics para su posterior uso de las políticas.

2. Alcance

Aplicar en el GAD Municipal del Cantón Mejía, definida en los modelos y anexos que apoyan al resguardo de la información.

3. Definiciones

-Política- Conjunto de reglas, lineamientos que permiten gestionar la seguridad de la información dentro de una organización.

-Usuario Final. - el usuario final de un producto informático (bien sea hardware o software), es la persona a la que va destinada dicho producto una vez ha superado las fases de desarrollo correspondientes.

-Servidor. - Es un equipo informático que forma parte de una red y provee servicios a otros equipos cliente.

-Tics. - Tecnologías de la información y la comunicación.

-Equipo. - Se denomina equipo a todo bien o maquina necesaria para desarrollar cualquier operación dentro de un proceso productivo y a la cual se le desea seguir un historial de mantenimiento y utilización. Un equipo debe de ser montado en una ubicación técnica y puede poseer una ubicación técnica y puede poseer un alista de materiales asociada.

4. Documentos de referencia

No aplica.

5. Descripción de la Política

El equipo debe tener una imagen que tenga elación a la corporación o entidad.

Al iniciar la sesión correspondiente por parte del usuario la imagen corporativa debe estar en la pantalla.

5.1. Área de Tecnología

- El departamento de Tics llevara y mantendrá el proceso correspondiente al manejo del active directory, siendo ellos los encargados de solucionar cualquier problema o inconveniente que se presente en el mismo.
- Igualmente, cada Dirección o Unidad debe hacer el trámite corresponde o informar a su superior inmediato y al Departamento Tics, sobre cualquier novedad que se presente.
- En los equipos de cómputo no podrán los usuarios hacer cambio de pantalla ya que este será establecido por el administrador del departamento de redes.

5.2. Responsabilidad de los Usuarios

- El hardware que se encuentra en el área de servidores y los armarios de comunicaciones es responsabilidad directa del personal del Departamento de TI, que tendrá que velar por su uso y cuidado.
- Los otros equipos de cómputo quedan bajo la responsabilidad del usuario al que se asignen. Estos tendrán la obligación de cuidarlos, mantenerlos limpios y velar por su buen funcionamiento. En el caso de existir algún problema con el equipo deberán de reportarlo inmediatamente al Departamento de TI para que se proceda a su revisión.
- Queda entendido que los recursos informáticos asignados a cada usuario lo serán en calidad de herramientas de trabajo; como tal se encuentra permanentemente bajo dominio y control del administrador del GAD, sin perjuicio del derecho a la privacidad de la información almacenada y demás derechos fundamentales establecidos por la Constitución Política.

16.3. Anexo 3: Política al presionar las teclas especiales

	POLÍTICA AL PRESIONAR LAS TECLAS ESPECIALES	PO-2S
		Ver No. 01
		Pág. 1 de 2

1. Objetivo

Definir e implementar lineamientos al presionar teclas especiales para el acceso al equipo, con respecto a la información que se presente al momento de que el usuario haga uso del mismo, mediante la recopilación de información en el departamento de tics para su posterior uso de las políticas.

2. Alcance

Aplicar las políticas de manera adecuada en el GAD Municipal del Cantón Mejía, definida en el documento.

3. Definiciones

-Política- Conjunto de reglas, lineamientos que permiten gestionar la seguridad de la información dentro de una organización.

-Usuario Final. - el usuario final de un producto informático (bien sea hardware o software), es la persona a la que va destinada dicho producto una vez ha superado las fases de desarrollo correspondientes.

-Servidor. - Es un equipo informático que forma parte de una red y provee servicios a otros equipos cliente.

-Tics. - Tecnologías de la información y la comunicación.

-Equipo. - Se denomina equipo a todo bien o maquina necesaria para desarrollar cualquier operación dentro de un proceso productivo y a la cual se le desea seguir un historial de mantenimiento y utilización. Un equipo debe de ser montado en una ubicación técnica y puede poseer una ubicación técnica y puede poseer un alista de materiales asociada.

-Teclas especiales. - Dicho de otra manera, todas las telas que no sean números o letras, forman parte del conjunto de teclas especiales, como ALT, CTRL, las telas de función, hotkeys, etc.

4. Documentos de referencia

No aplica.

5. Descripción de la Política

El usuario podrá hacer uso de las teclas especiales tales como Ctrl+Alt+Supr para el ingreso de usuario y contraseña.

Al iniciar la sesión con la utilización de las teclas especiales el usuario deberá ingresar su correspondiente contraseña.

5.1. Área de Tecnología

- El departamento de Tics llevara y mantendrá el proceso correspondiente al manejo del active directory, siendo ellos los encargados de solucionar cualquier problema o inconveniente que se presenta en el mismo.
- Igualmente, cada Dirección o Unidad debe hacer el trámite correspondiente o informar a su superior inmediato y al departamento Tics sobre cualquier novedad que se presente.
- En los equipos de cómputo no podrán los usuarios hacer ningún cambio de pantalla ya que este será establecido por el administrador del departamento de redes.

5.2. Responsabilidad de los usuarios

- El hardware que se encuentra en el área de servidores y los armarios de comunicaciones es responsabilidad directa del personal del Departamento de TI, que tendrá que velar por su uso y cuidado.
- Los otros equipos de cómputo quedan bajo la responsabilidad del usuario al que se asignen. Estos tendrán la obligación de cuidarlos, mantenerlos limpios y velar por su buen funcionamiento. En el caso de existir algún problema con el equipo deberán de reportarlo inmediatamente al Departamento de TI para que se proceda a su revisión.
- Queda entendido que los recursos informáticos asignados a cada usuario lo serán en calidad de herramientas de trabajo; como tal se encuentra permanentemente bajo dominio y control del administrador del GAD.

16.4. Anexo 4: Política fondo de pantalla

	POLÍTICA FONDO DE PANTALLA	PO-3F
		Ver No. 01
		Pág. 1 de 2

1. Objetivo

Definir e implementar lineamientos del fondo de pantalla del equipo, con respecto a la información que se presente al momento de que el usuario haga uso del mismo, mediante la recopilación de información en el departamento de tics para su posterior uso de las políticas.

2. Alcance

Aplicar las políticas de manera adecuada en el GAD Municipal del Cantón Mejía, para un mejor proceso.

3. Definiciones

-Política- Conjunto de reglas, lineamientos que permiten gestionar la seguridad de la información dentro de una organización.

-Usuario Final. - el usuario final de un producto informático (bien sea hardware o software), es la persona a la que va destinada dicho producto una vez ha superado las fases de desarrollo correspondientes.

-Servidor. - Es un equipo informático que forma parte de una red y provee servicios a otros equipos cliente.

-Tics. - Tecnologías de la información y la comunicación.

-Equipo. - Se denomina equipo a todo bien o maquina necesaria para desarrollar cualquier operación dentro de un proceso productivo y a la cual se le desea seguir un historial de mantenimiento y utilización. Un equipo debe de ser montado en una ubicación técnica y puede poseer una ubicación técnica y puede poseer un alista de materiales asociada.

4. Documentos de referencia

No aplica.

5. Descripción de la política

Al iniciar la sesión aparecerá un fondo de pantalla la cual será automática.

Al iniciar la sesión correspondiente por parte del usuario el fondo de pantalla será automático y de la corporación.

5.1. Área de Tecnología

- El departamento de Tics llevara y mantendrá el proceso correspondiente al manejo del active directory, siendo ellos los encargados de solucionar cualquier problema o inconveniente que se presenta en el mismo.
- Igualmente, cada Dirección o Unidad debe hacer el trámite correspondiente o informar a su superior inmediato y al departamento Tics sobre cualquier novedad que se presente.
- En los equipos de cómputo no podrán los usuarios hacer ningún cambio de pantalla ya que este será establecido por el administrador del departamento de redes.

5.2.Responsabilidad de los usuarios

- El hardware que se encuentra en el área de servidores y los armarios de comunicaciones es responsabilidad directa del personal del Departamento de TI, que tendrá que velar por su uso y cuidado.
- Los otros equipos de cómputo quedan bajo la responsabilidad del usuario al que se asignen. Estos tendrán la obligación de cuidarlos, mantenerlos limpios y velar por su buen funcionamiento. En el caso de existir algún problema con el equipo deberán de reportarlo inmediatamente al Departamento de TI para que se proceda a su revisión.
- Queda entendido que los recursos informáticos asignados a cada usuario lo serán en calidad de herramientas de trabajo; como tal se encuentra permanentemente bajo dominio y control del administrador del GAD, sin perjuicio del derecho a la privacidad de la información almacenada y demás derechos fundamentales establecidos por la Constitución Política.

16.5. Anexo 5: Política tres veces ingresada mal la contraseña se bloquea

	POLÍTICA TRES VECES INGRESADA MAL LA CONTRASEÑA SE BLOQUEA	PO-4T
		Ver No. 01
		Pág. 1 de 2

1. Objetivo

Definir e implementar lineamientos de seguridad con respecto al bloqueo de contraseña `pasado los tres intentos, con respecto a la información que se presente al momento de que el usuario haga uso del mismo, mediante la recopilación de información en el departamento de tics para su posterior uso de las políticas.

2. Alcance

Aplicar en el GAD Municipal del Cantón Mejía, definida en los modelos que apoyan al resguardo de la información.

3. Definiciones

-Política- Conjunto de reglas, lineamientos que permiten gestionar la seguridad de la información dentro de una organización.

-Usuario Final. - el usuario final de un producto informático (bien sea hardware o software), es la persona a la que va destinada dicho producto una vez ha superado las fases de desarrollo correspondientes.

-Servidor. - Es un equipo informático que forma parte de una red y provee servicios a otros equipos cliente.

-Tics. - Tecnologías de la información y la comunicación.

-Equipo. - Se denomina equipo a todo bien o maquina necesaria para desarrollar cualquier operación dentro de un proceso productivo y a la cual se le desea seguir un historial de mantenimiento y utilización. Un equipo debe de ser montado en una ubicación técnica y puede poseer una ubicación técnica y puede poseer un alista de materiales asociada.

4. Documentos de referencia

No aplica.

5. Descripción de la Política

- Cuando el usuario ingrese por tercera vez mal contraseña la máquina se bloqueará automáticamente.
- No tendrá acceso a su cuenta del equipo por lo que deberá acercarse al administrador de tics y pedir una nueva contraseña.

5.1. Área de Tecnología

- El departamento de Tics llevara y mantendrá el proceso correspondiente al manejo del active directory, siendo ellos los encargados de solucionar cualquier problema o inconveniente que se presenta en el mismo.
- Igualmente, cada Dirección o Unidad debe hacer el trámite correspondiente o informar a su superior inmediato y al departamento Tics sobre cualquier novedad que se presente.
- En los equipos de cómputo no podrán los usuarios hacer ningún cambio de pantalla ya que este será establecido por el administrador del departamento de redes.

5.2.Responsabilidad de los Usuarios

- Los otros equipos de cómputo quedan bajo la responsabilidad del usuario al que se asignen. Estos tendrán la obligación de cuidarlos, mantenerlos limpios y velar por su buen funcionamiento. En el caso de existir algún problema con el equipo deberán de reportarlo inmediatamente al Departamento de TI para que se proceda a su revisión.
- Queda entendido que los recursos informáticos asignados a cada usuario lo serán en calidad de herramientas de trabajo; como tal se encuentra permanentemente bajo dominio y control del administrador del GAD, sin perjuicio del derecho a la privacidad de la información almacenada y demás derechos fundamentales establecidos por la Constitución Política.
- El usuario deberá ser responsable con la contraseña que le asigne, caso contrario podría tener problemas si se le olvidara ya que el equipo solo le permite ingresar tres veces la clave.

16.6. Anexo 6: Política cinco minutos de inactividad se bloquea

	POLÍTICA CINCO MINUTOS DE INACTIVIDAD SE BLOQUEA	PO-5M
		Ver No. 01
		Pág. 1 de 2

1. Objetivo

Definir e implementar lineamientos de la inactividad del equipo, con respecto a la información que se presente al momento de que el usuario haga uso del mismo, mediante la recopilación de información en el departamento de tics para su posterior uso de las políticas.

2. Alcance

Aplicar en el GAD Municipal del Cantón Mejía, definida en los modelos y anexos que apoyan al resguardo de la información.

3. Definiciones

-Política- Conjunto de reglas, lineamientos que permiten gestionar la seguridad de la información dentro de una organización.

-Usuario Final.- el usuario final de un producto informático (bien sea hardware o software), es la persona a la que va destinada dicho producto una vez ha superado las fases de desarrollo correspondientes.

-Servidor.- Es un equipo informático que forma parte de una red y provee servicios a otros equipos cliente.

-Tics.- Tecnologías de la información y la comunicación.

-Equipo.- Se denomina equipo a todo bien o maquina necesaria para desarrollar cualquier operación dentro de un proceso productivo y a la cual se le desea seguir un historial de mantenimiento y utilización. Un equipo debe de ser montado en una ubicación técnica y puede poseer una ubicación técnica y puede poseer un alista de materiales asociada.

-Inactividad.- Falta de actividad o de movimiento.

4. Documentos de referencia

No aplica.

5. Descripción de la Política

En el momento que el usuario ingrese al equipo con su respectiva contraseña, y no haga uso del mismo, después de 5 minutos de inactividad deberá volver a ingresar los datos.

El equipo después de los 5 minutos deberá cerrar la sesión automáticamente y el usuario deberá ingresar las credenciales correspondientes.

5.1. Área de Tecnología

- El departamento de Tics llevara y mantendrá el proceso correspondiente al manejo del active directory, siendo ellos los encargados de solucionar cualquier problema o inconveniente que se presenta en el mismo.
- Igualmente, cada Dirección o Unidad debe hacer el trámite correspondiente o informar a su superior inmediato y al departamento Tics sobre cualquier novedad que se presente.

5.2. Responsabilidad de los Usuarios

- El hardware que se encuentra en el área de servidores y los armarios de comunicaciones es responsabilidad directa del personal del Departamento de TI, que tendrá que velar por su uso y cuidado.
- Los otros equipos de cómputo quedan bajo la responsabilidad del usuario al que se asignen. Estos tendrán la obligación de cuidarlos, mantenerlos limpios y velar por su buen funcionamiento. En el caso de existir algún problema con el equipo deberán de reportarlo inmediatamente al Departamento de TI para que se proceda a su revisión.
- Queda entendido que los recursos informáticos asignados a cada usuario lo serán en calidad de herramientas de trabajo; como tal se encuentra permanentemente bajo dominio y control del administrador del GAD, sin perjuicio del derecho a la privacidad de la información almacenada y demás derechos fundamentales establecidos por la Constitución Política.
- El usuario deberá ser responsable con la contraseña que le asigne, caso contrario podría tener problemas si se le olvidara ya que el equipo solo le permite ingresar tres veces la clave.

16.7. Anexo 7: Política actualización de contraseña

	POLÍTICA ACTUALIZACION DE CONTRASEÑA	PO-6A
		Ver No. 01
		Pág. 1 de 2

1. Objetivo

Definir e implementar lineamientos de seguridad con la actualización de la contraseña de todo el municipio cada tres meses, con respecto a la información que se presente al momento de que el usuario haga uso del mismo, mediante la recopilación de información en el departamento de tics para su posterior uso de las políticas.

2. Alcance

Aplicar en el GAD Municipal del Cantón Mejía, definida en los modelos y anexos que apoyan al resguardo de la información.

3. Definiciones

-Política- Conjunto de reglas, lineamientos que permiten gestionar la seguridad de la información dentro de una organización.

-Usuario Final.- el usuario final de un producto informático (bien sea hardware o software), es la persona a la que va destinada dicho producto una vez ha superado las fases de desarrollo correspondientes.

-Servidor.- Es un equipo informático que forma parte de una red y provee servicios a otros equipos cliente.

-Tics.- Tecnologías de la información y la comunicación.

-Equipo.- Se denomina equipo a todo bien o maquina necesaria para desarrollar cualquier operación dentro de un proceso productivo y a la cual se le desea seguir un historial de mantenimiento y utilización. Un equipo debe de ser montado en una ubicación técnica y puede poseer una ubicación técnica y puede poseer un alista de materiales asociada.

4. Documentos de referencia

No aplica.

5. Descripción de la Política

La contraseña de todo el personal del municipio se deberá actualizar cada tres meses por seguridad de la corporación y del personal.

Esta política será de manera obligatoria para el municipio en general.

Solo el administrador del área de tics podrá realizar los cambios pertinentes en el periodo acordado.

5.1.Área de Tecnología

- El departamento de Tics llevara y mantendrá el proceso correspondiente al manejo del active directory, siendo ellos los encargados de solucionar cualquier problema o inconveniente que se presenta en el mismo.
- Igualmente, cada Dirección o Unidad debe hacer el trámite correspondiente o informar a su superior inmediato y al departamento Tics sobre cualquier novedad que se presente.

5.2. Responsabilidad de los Usuarios

- El hardware que se encuentra en el área de servidores y los armarios de comunicaciones es responsabilidad directa del personal del Departamento de TI, que tendrá que velar por su uso y cuidado.
- Los otros equipos de cómputo quedan bajo la responsabilidad del usuario al que se asignen. Estos tendrán la obligación de cuidarlos, mantenerlos limpios y velar por su buen funcionamiento. En el caso de existir algún problema con el equipo deberán de reportarlo inmediatamente al Departamento de TI para que se proceda a su revisión.
- Queda entendido que los recursos informáticos asignados a cada usuario lo serán en calidad de herramientas de trabajo; como tal se encuentra permanentemente bajo dominio y control del administrador del GAD, sin perjuicio del derecho a la privacidad de la información almacenada y demás derechos fundamentales establecidos por la Constitución Política.

16.8. Anexo 8. Manual de Usuario para la Administración del Active Directory

Manual de Usuario para la Administración del Active Directory

Objetivo:

Disponer de un manual de usuario para la administración del servicio del directorio Active Directory de Microsoft Windows Server 2012, para poder tener una buena gestión de las cuentas de dominio.

Introducción:

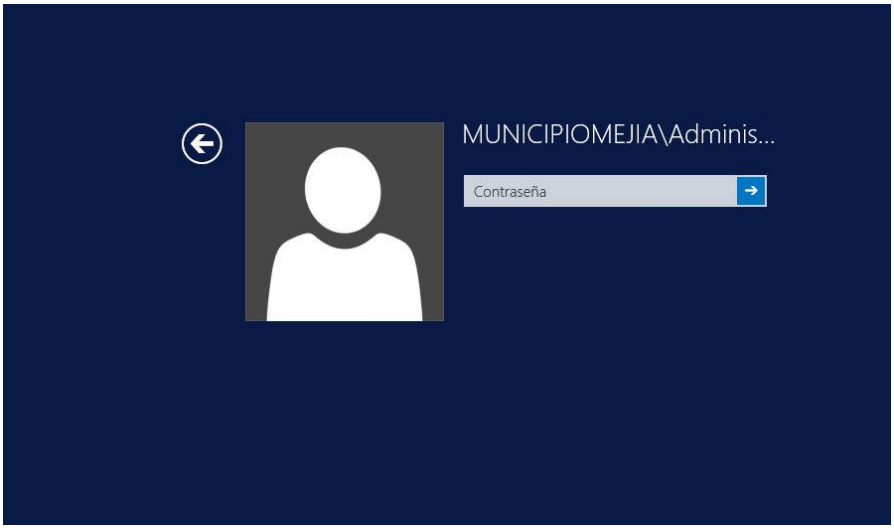
Este documento es una breve introducción a la administración del Active Directory y de los complementos de usuarios y equipos que trae el servidor Active Directory de Microsoft Windows Server 2012.

Este complemento nos permitirá agregar, mover, eliminar y modificar las propiedades de los objetos que tiene el Active Directory como usuarios, unidades organizacionales, equipos y grupos.

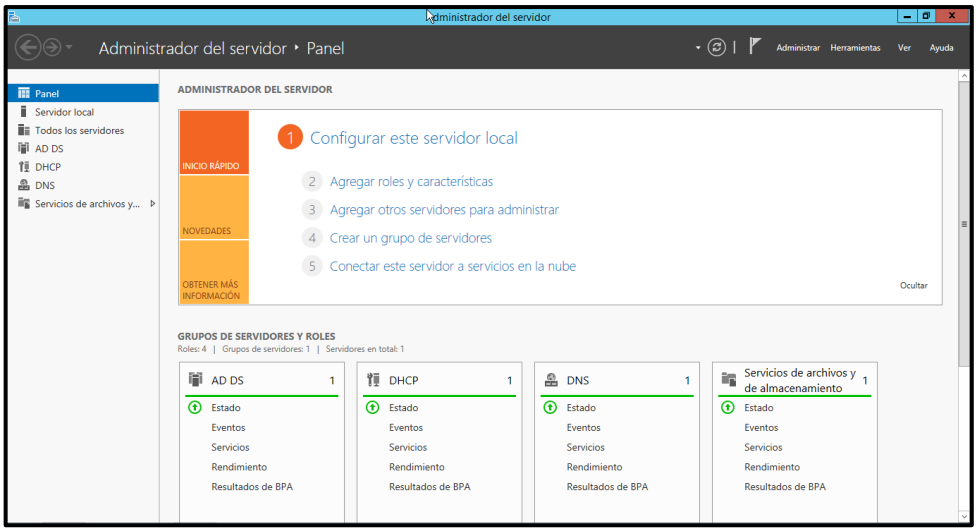
Desarrollo:

Ingreso al Active Directory

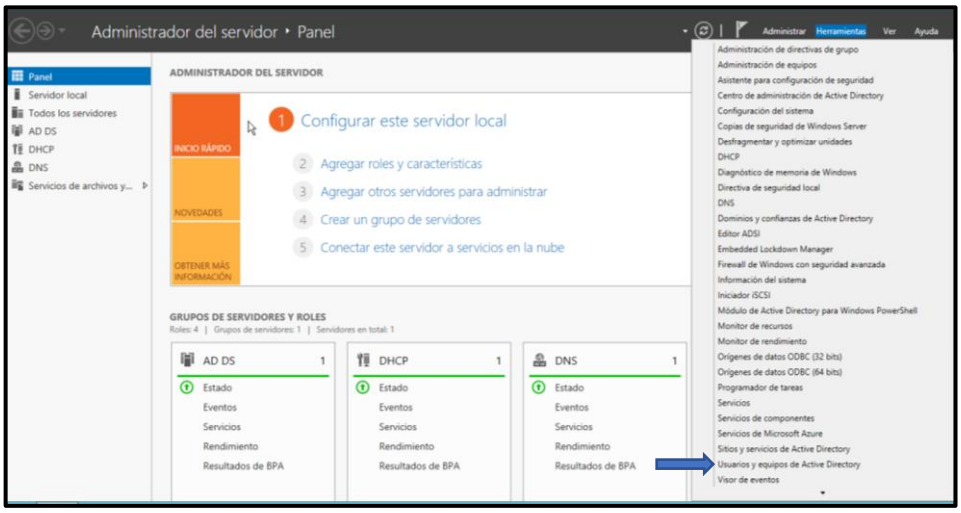
Encendemos la máquina que tiene el servidor Active Directory, y lo que debemos presionar es CTRL+ALT+SUPR, e iniciamos sesión en el servidor como administrador e ingresamos la clave y pulsamos Aceptar.



Al momento que ya ingresamos la clave nos va a aparecer la pantalla principal, con la pantalla de Administrador del Servidor en donde podemos ver que se encuentran instalados los servidores DNS y DHCP



Hacemos clic en la pestaña Herramientas que se encuentra dentro del Administrador del servidor y escogemos la opción “Usuarios y Equipos del Active Directory”



Una vez que ingresemos vamos ha observar muchos objetos los cuales voy a describir en la siguiente tabla la cual aparece por defecto en la creación del Active Directory.

CARPETA	DESCRIPCIÓN
Domain	Este es un complemento que representa el dominio administrativo en nuestro caso el dominio es **municipiomejia.gob**
Builtin	Nos permite tener información de grupos administrativos que se han creado de forma automática.

Computers	Nos permite contener todos los equipos que posee Windows 8, Windows 10, que se unen a nuestro dominio.
Users	Contiene grupos administrativos que se han creado automáticamente en la carpeta de usuarios.

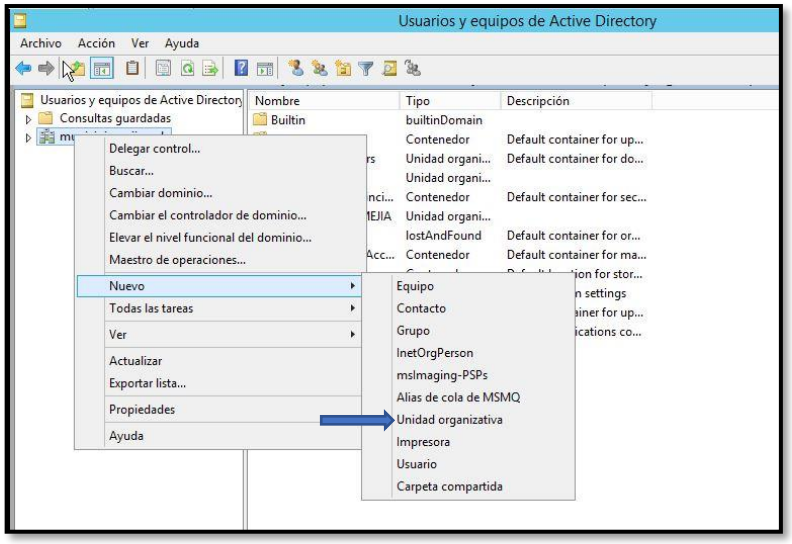
Se puede usar Active Directory para crear los siguientes objetos:

OBJETO	**DESCRIPCIÓN**
Equipo	Esto representa a un equipo en la red.
Contacto	Es una cuenta que no tiene ningún permiso de seguridad. No se puede iniciar una sesión como contacto.
Grupo	Los grupos pueden contener usuarios, equipos y otros grupos. Nos permiten administrar las cantidades grandes de objetos.
Unidad organizativa	La unidad organizativa nos permite organizar de manera lógica los objetos del directorio.
Impresora	Permite tener impresoras en la red.
Usuario	Los usuarios se crean al momento que debemos ingresar una computadora al dominio.
Carpeta compartida	Es un recurso compartido de red.

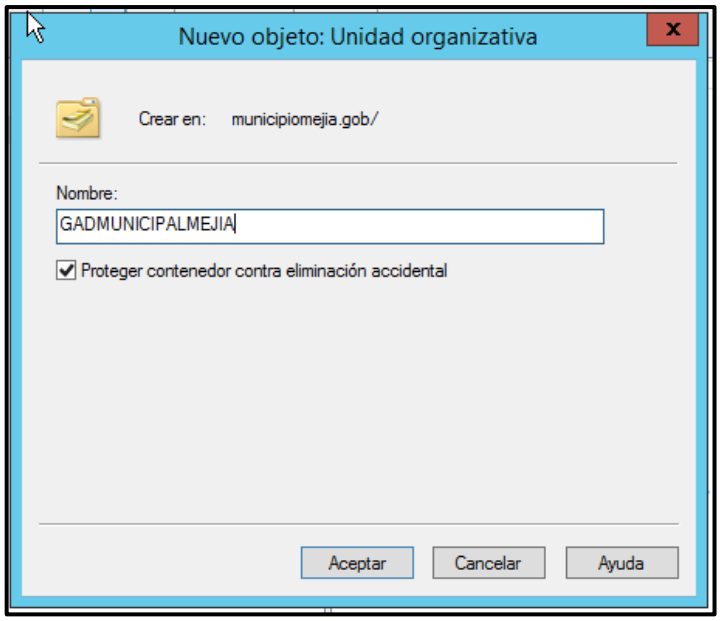
Una vez que tenemos claro cuales objetos podemos crear y cuales vienen por defecto al momento de instalar el Active Directory vamos a proceder con la creación de unidades organizativas.

Crear unidades organizativas

1. Para esto debemos dar clic derecho del mouse en el nombre del dominio, seleccionamos Nuevo, y hacemos clic en “Unidades organizativas”.

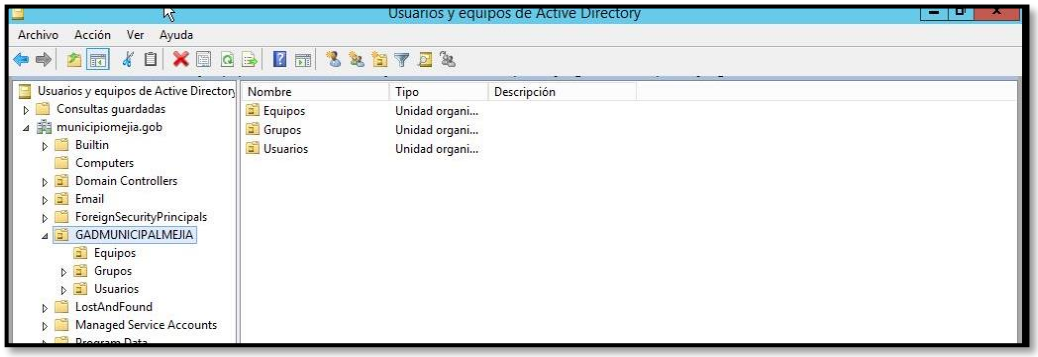


2. Introducimos el nombre de la unidad organizativa según la organización o la infraestructura que dicte la dirección, luego damos clic en Aceptar.



Al momento que poner Aceptar vamos a ver como se crea la unidad organizativa.

3. Después de haber creado la unidad organizativa raíz debemos dividirlos en 3 categorías las cuales son: Usuarios, Equipos y Grupos en las cuales se van a almacenar los datos.



Crear cuenta de usuario

Para poder crear las cuentas de usuario debemos tener en cuenta estos aspectos:

- A que Categoría de la unidad organizativa pertenece dependiendo de la organización del GAD Municipal del Cantón Mejía.
- Los nombres de los usuarios deben ser únicos.

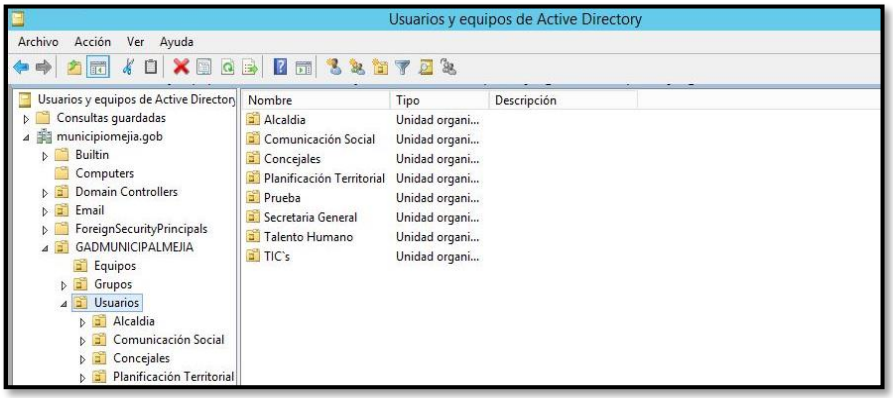
En este caso debido a las políticas que utiliza el GAD Municipal del Cantón Mejía el formato para crear los nombres de los usuarios es la inicial del primer nombre seguida de un punto y el primer apellido. Ejemplo:

Jorge Santiago Espinel Pilicita	j.espinel
María Belén Collaguazo Quinatoa	m.collaguazo
Diana Nataly Toapanta Chilig	d.toapanta

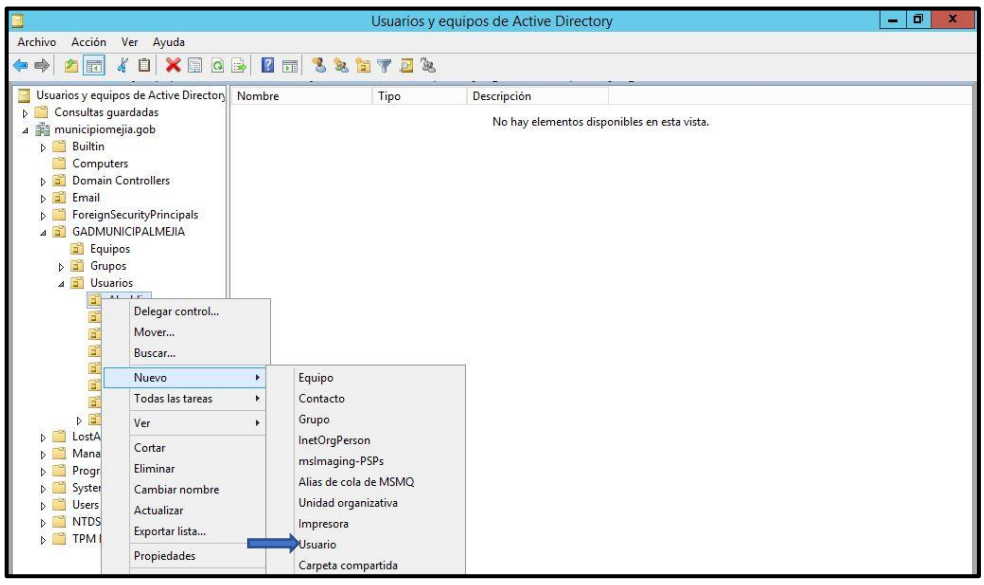
Si existen usuarios duplicados el nombre debemos utilizar la inicial del primer y del segundo nombre seguida del punto y apellido paterno como lo podemos observar.

Diana Raquel Toapanta Caiza	dr.toapanta
María Ester Collaguazo Lopez	me.collaguazo

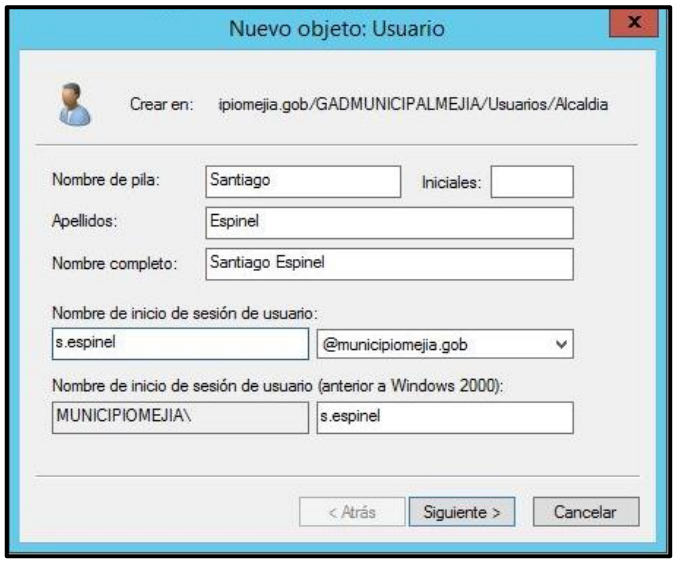
1. Para la creación de usuarios vamos a la unidad organizacional: Usuarios en donde vamos a crear subcategorías las cuales van a ser nombradas con cada uno de los departamentos que posee el GAD Municipal del Cantón Mejía.



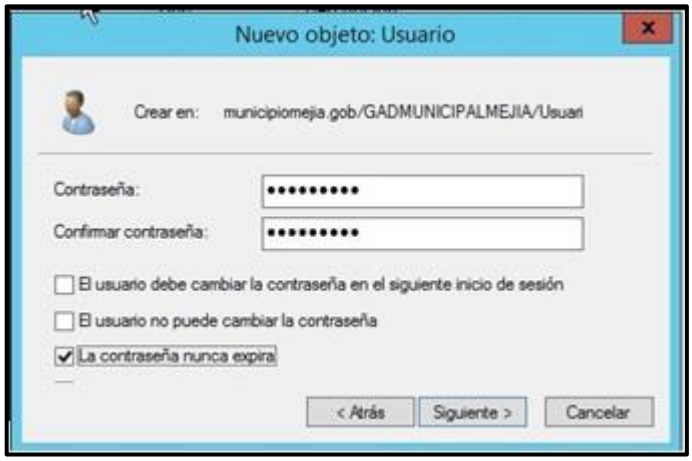
2. Damos clic derecho en la unidad organizativa de los departamentos del GAD Municipal del Cantón Mejía, vamos a nuevo y a continuación hacemos clic en Usuario.



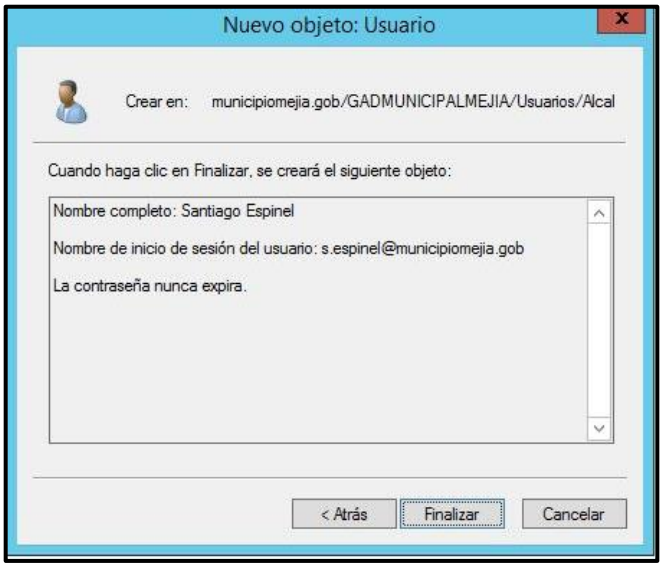
3. Debemos llenar los campos que nos aparecen, y luego dar clic en Siguiente:



4. Nos muestra una pantalla nueva en donde nos dice que ingresemos una contraseña para la cuenta del usuario y luego en siguiente.



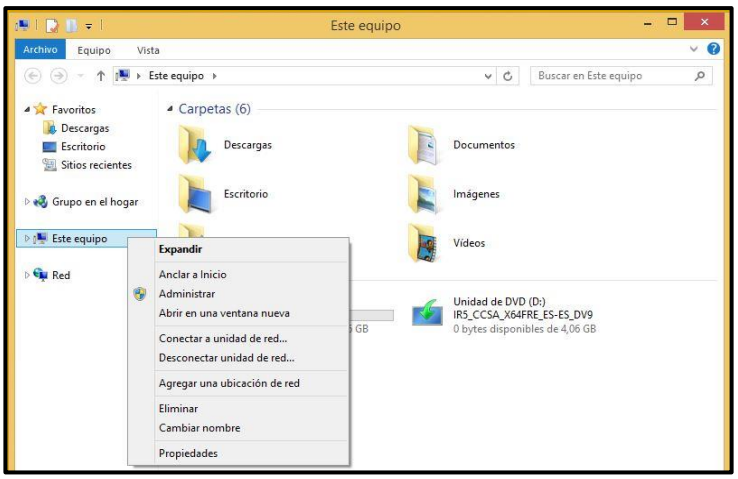
5. Hacemos clic en finalizar. Así es como creamos las cuentas de usuarios en las unidades organizativas.



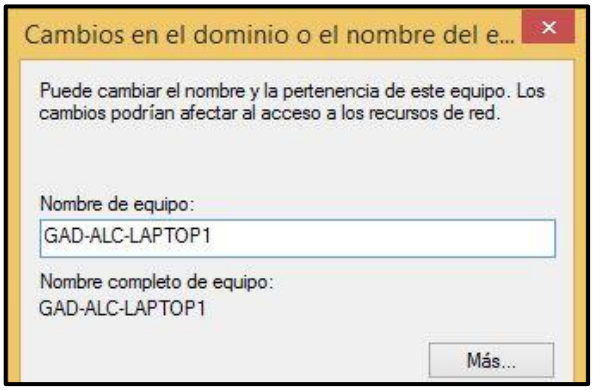
Agregar un equipo al dominio

Para unir a un cliente al dominio, deberemos hacer iniciar sesión en la computadora.

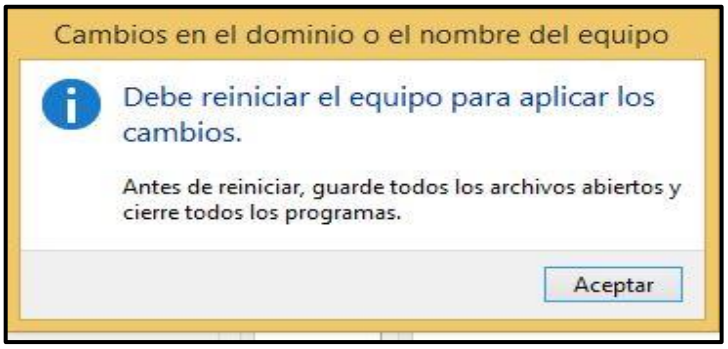
1. Una vez dentro del computador del usuario vamos al icono de MI PC y luego en propiedades.



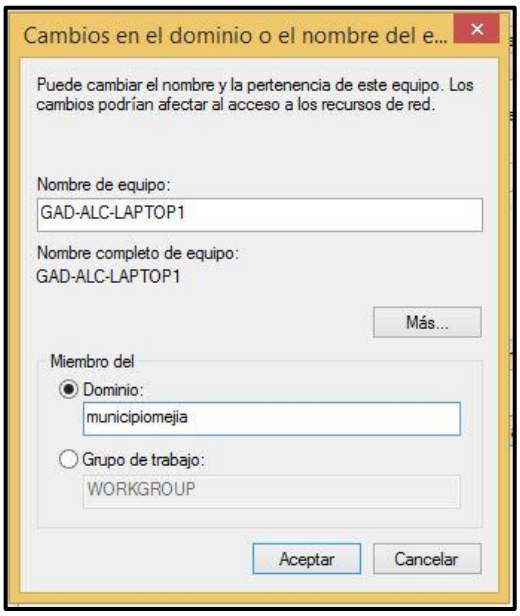
2. Primero debemos cambiar el nombre del equipo dependiendo del departamento que se encuentre, debemos nombrarles así: entidad – iniciales del departamento – tipo y # Computadora ejemplo: GAD-ALC-LAPTOP1.

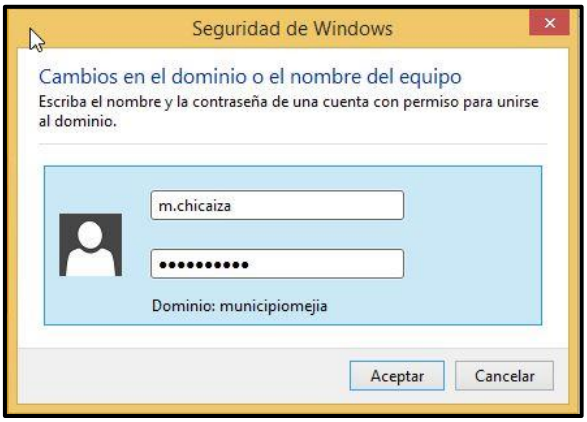


3. Luego de cambiar el nombre del equipo se va a reiniciar, damos clic derecho en Mi PC, propiedades, cambiar configuraciones, y en cambiar.

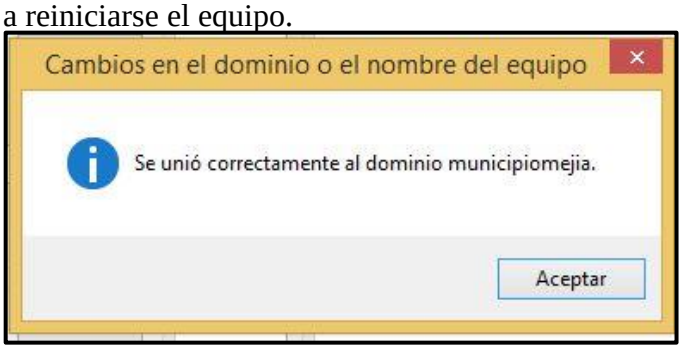


4. Seleccionamos e introducimos el nombre del dominio en este caso sería (**municipiomejia**), luego damos clic en Aceptar, nos aparecerá que ingresemos el usuario y la contraseña.





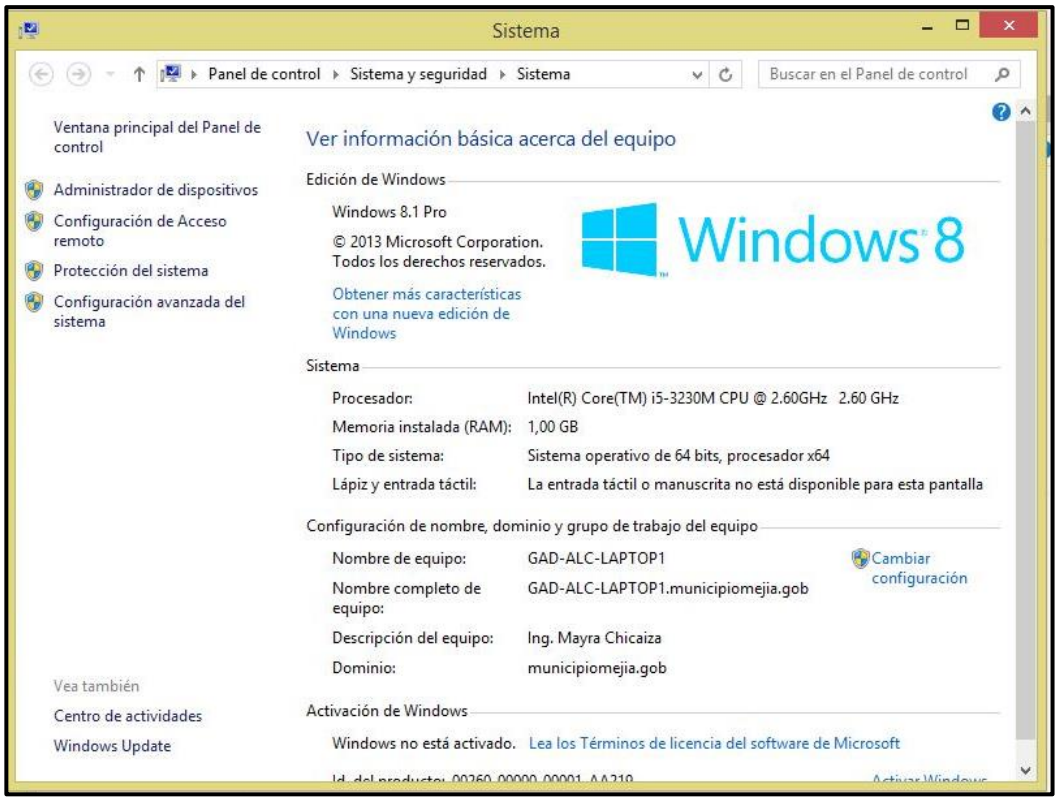
5. Tras unos segundos, se nos dará la bienvenida al dominio, debemos dar clic en Aceptar y comenzará a reiniciarse el equipo.



Una vez reiniciado el equipo nos pedirá que iniciemos la sesión del usuario.

6. En este caso nos aparecerá una pantalla para que ingresemos la contraseña, al momento de darle CTRL + ALT + SUPR, procedemos a ingresar el usuario y la contraseña.

7. Si se encuentra bien configurado la unión del servidor con el usuario, la sesión ya está lista para ser utilizada, para poder comprobar que se encuentra en el dominio, vamos a MI PC, y seleccionamos las propiedades.



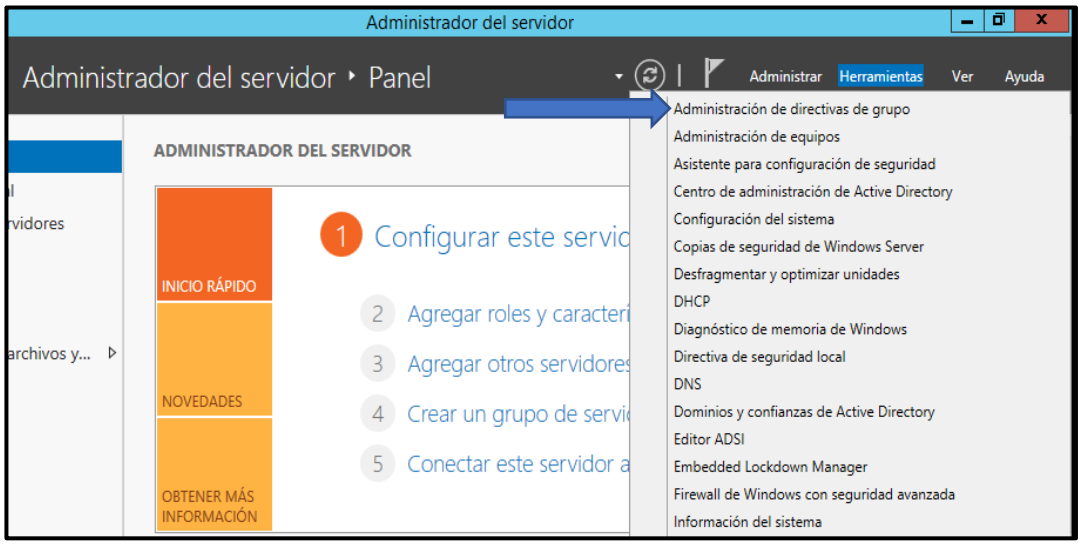
<u>Como añadir Políticas de seguridad</u>

Las GPO nos permiten tener una buena administración de los objetos de usuarios y equipos que se encuentran dentro del Active Directory.

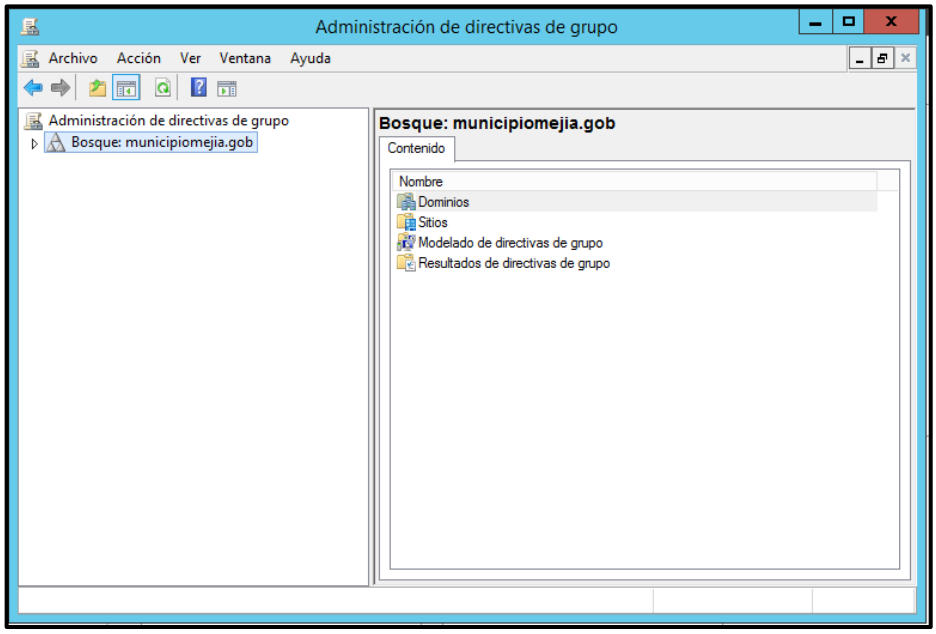
Para poder insertar las políticas debemos saber cuáles son las diferencias de los distintos niveles y ponerlos configurar.

- Equipo Local: Esta GPO se aplicará únicamente al equipo que tengas asignado.
- Sitio: Los GPO se aplicarán a los equipos y usuarios que estén dentro de un sitio, independiente del dominio.
- Dominio: Las GPO se aplicarán a todos los equipos y usuarios que pertenecen al dominio.
- Unidad Organizativa: Se aplicará únicamente a los equipos y usuarios que estén dentro o pertenezcan a esa Unidad organizacional.

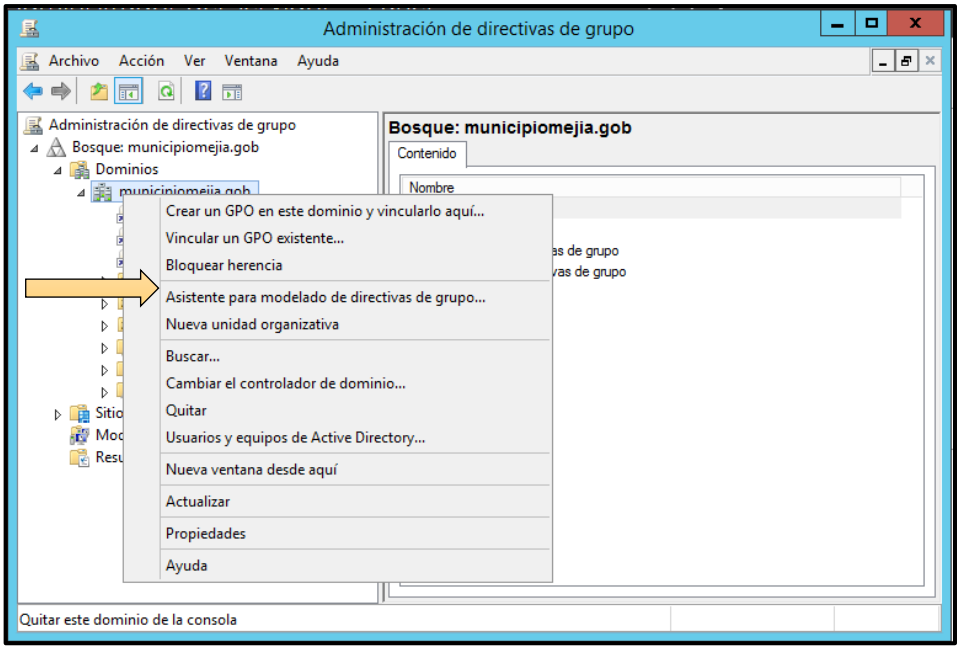
1. Para poder insertar las políticas primero debemos ir al servidor de dominio y en la pantalla principal de debemos dar clic en la opción “Administración de directivas de grupo”.



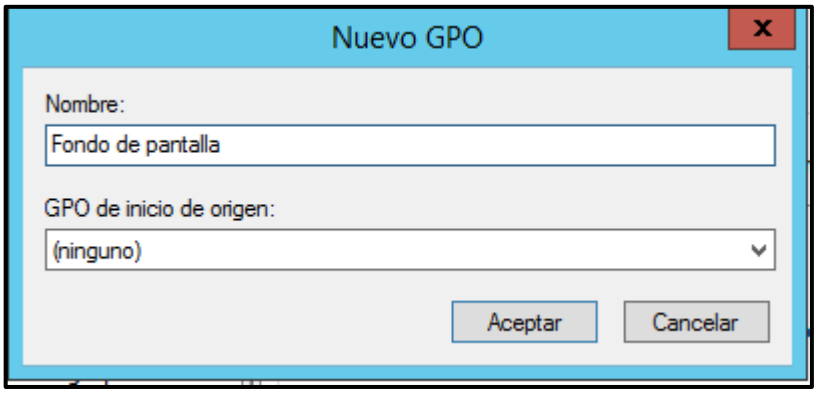
2. Se nos va a abrir una pantalla nueva en la cual nos muestra el nombre del dominio.



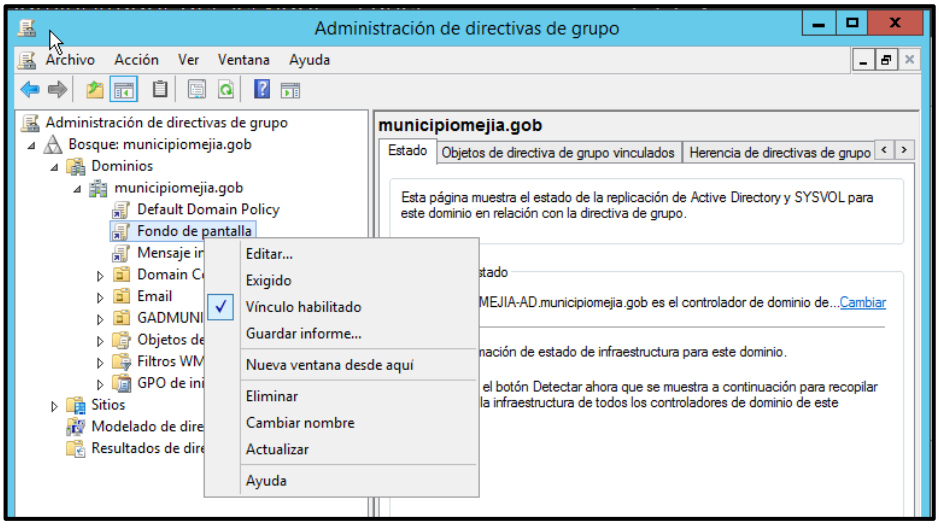
3. Damos un clic derecho en donde vayamos a crear la GPO, y seleccionamos “Crear un GPO en este dominio y vincularlo aquí…”



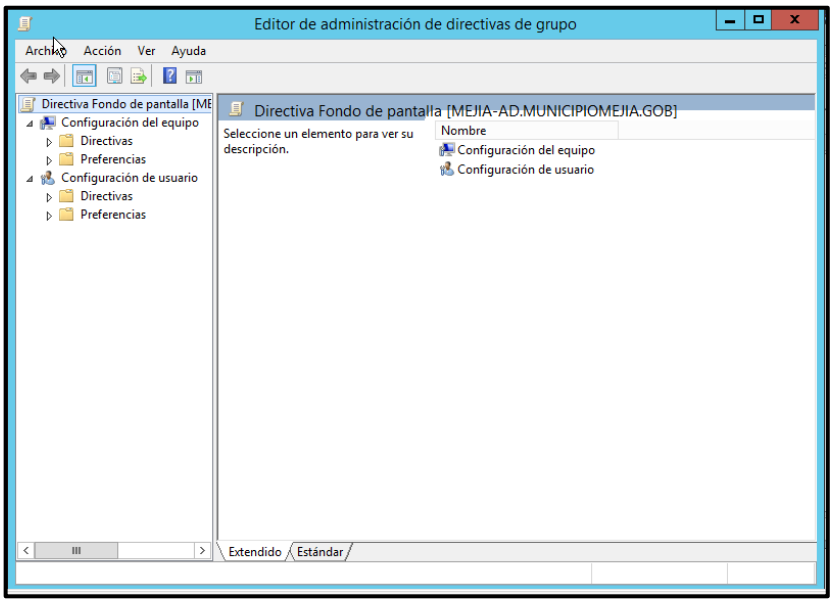
4. Al momento que damos clic en esa opción nos aparece una ventana en donde nos dice que ingresemos el nombre de la GPO.



5. Al momento de poner Aceptar el GPO ya se coloca en la lista en donde vamos a dar un clic derecho para poder configurar.



6. Y al final nos aparecerá otra ventana nueva en donde deberemos configurar, para la mayoría de los GPO nos va a salir la mima pantalla solo hay que saber como configurar para cada una de ellas.



MANUAL DEL CORREO ZIMBRA

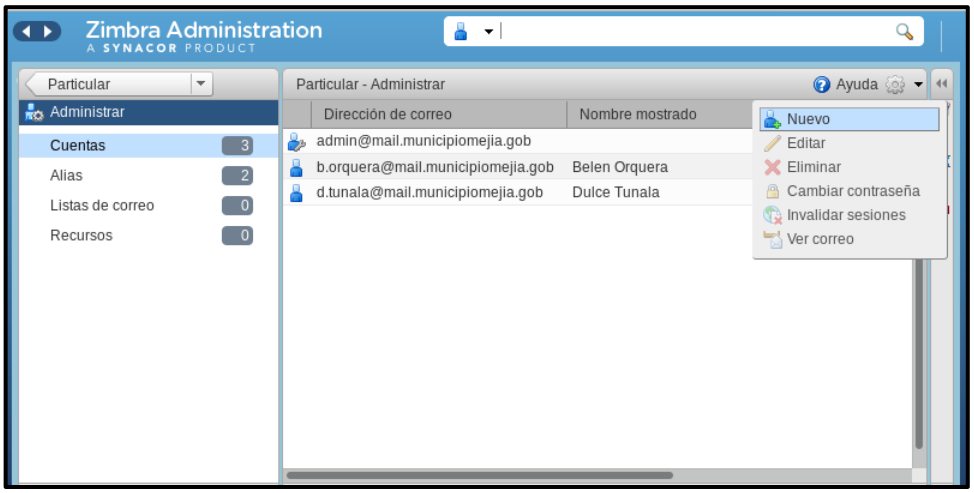
Correo Electrónico Administrador Zimbra

A continuación se detalla los pasos que se debe seguir para el manejo del correo Administrador Zimbra:

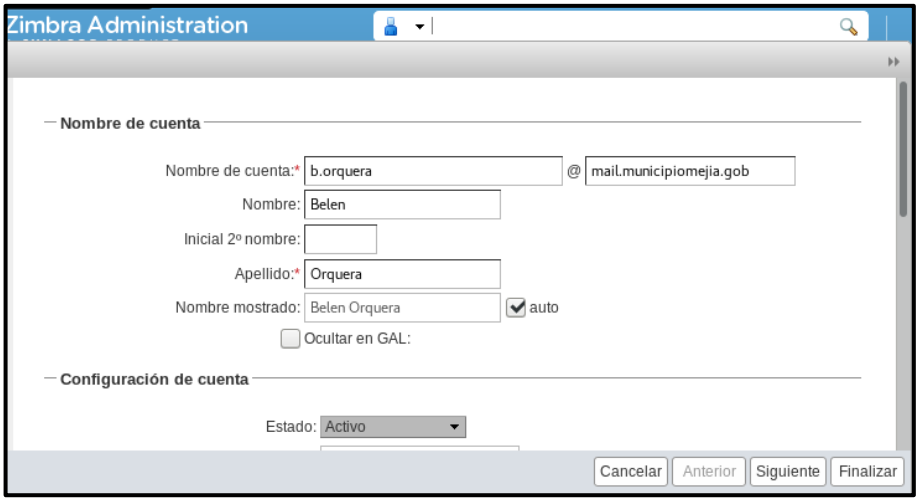
1. Ingresar a la URL **https://192.168.0.10:7071**
   - Usuario y contraseña del Administrador

2. Una vez dentro del correo Zimbra vamos a las opción Administrar que se encuentra en la parte izquierda, esto no lleva administrar las cuentas. Para realizar una nueva cuenta

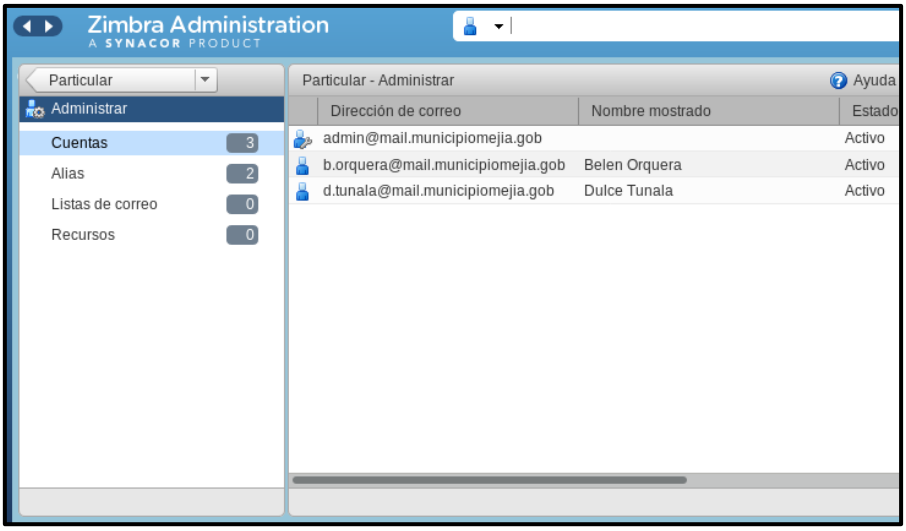
lo que hacemos es dirigirnos a la pestaña triangular que se encuentra en la parte superior derecha le damos clic en nuevo, para proceder a crear un nuevo usuario en el Zimbra.



3. Se debe llenar todos los campos vacíos, en cada campo lo que se debe poner son los datos del usuario a ser creado, cabe recalcar que no habrá un campo para la contraseña, ya que será creado desde el active directory.



4. Una vez llenado los campos lo que se hace es dar clic en Finalizar y entonces la cuenta ya se encontrara creada. El administrador puede realizar las cuentas directamente desde el Active directory, ya que existe una sincronización de cuentas por lo que la contraseña es la misma y solo el Administrador puede cambiarla.

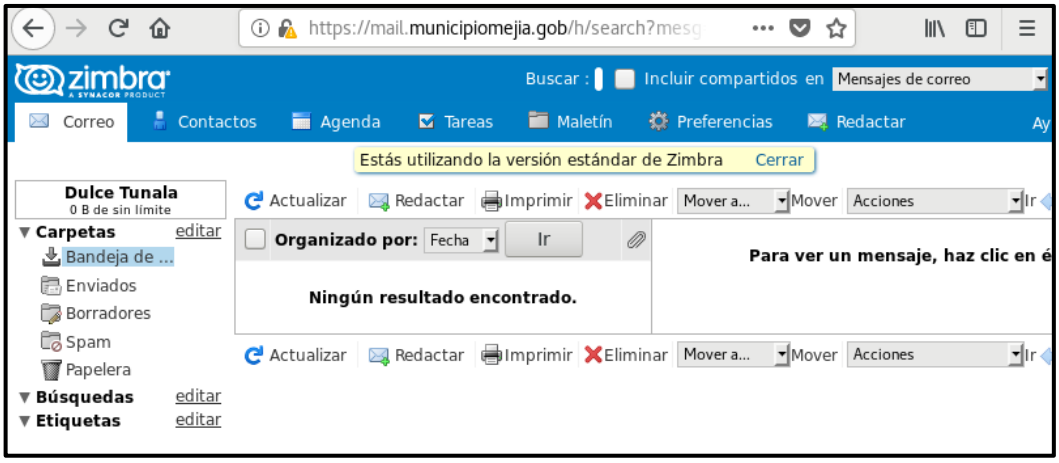


Correo Electrónico Cliente Zimbra

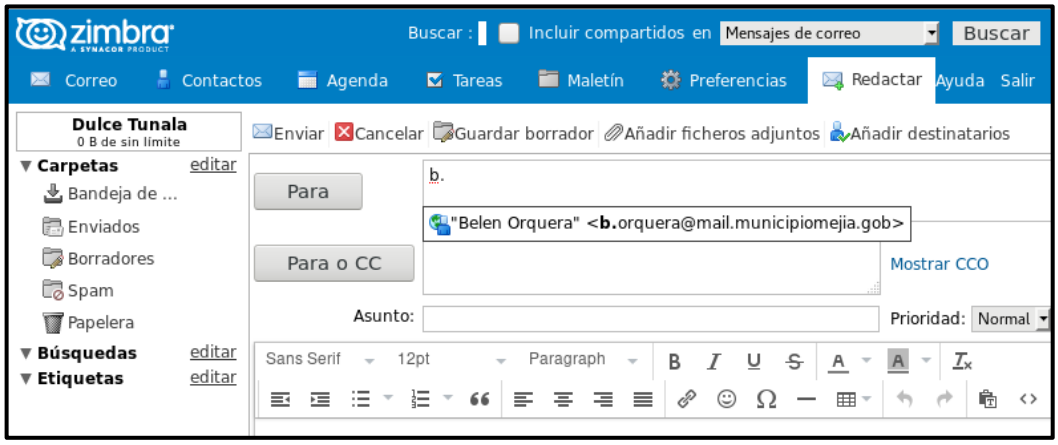
A continuación se detalla los pasos que se debe seguir para el manejo del correo Cliente Zimbra:

1. Ingresar a la URL **https://mail.municipiomejia.gob**
   - Usuario y contraseña
   - El nombre del usuario siempre será la primera letra del primer nombre, punto y el primer apellido seguido del nombre del dominio (Ejemplo: **d.tunala@mail.municipiomejia.gob**).
   - La contraseña será creada por el Administrador del Active Directory, la cual no se podrá cambiar ya que solo el Administrador podrá hacer esos cambios.

2. El uso del Cliente Zimbra es similar al de otras opciones de correo web, notaremos los conocidos Menús: Correo, Contactos, Agendas, Tareas, Maletín, etc.



✓ **Correo:** Se usa para enviar y recibir correos electrónicos, al redactar un nuevo mensaje nos muestra alternativas desde los Contactos corporativos, así como también los contactos personales agregados manualmente en la agenda.



3. Para salir deben ir a la parte superior derecha de la pantalla y hacer click en “Salir”.