Implementación de un controlador de dominio en la Comandancia General del Ejercito mediante un servidor activo basado en Opensource, para organizar, controlar y administrar de forma centralizada el acceso a los recursos de la red, y desarrollo: de los procedimientos y de las políticas para su administración, levantamiento de las políticas y manuales de administración aplicables a las particularidades de las direcciones que conforman la comandancia general del ejército.

Moncayo Sinchiguano, Flavio Rolando y Sánchez Changoluisa, Oscar Marcelo

Departamento de Eléctrica y Electrónica

Carrera de Tecnología Superior en Redes y Telecomunicaciones

Monografía, previo a la obtención del título de Tecnólogo Superior en Redes y Telecomunicaciones

Ing. Tintín Perdomo, Verónica Paulina

07 de marzo del 2022

DEPARTAMENTO DE ELÉCTRICA Y ELECTRÓNICA

CARRERA DE TECNOLOGÍA SUPERIOR EN REDES Y TELECOMUNICACIONES

CERTIFICACIÓN

Certifico que la monografía, "**Implementación de un controlador de dominio en la Comandancia General del Ejercito mediante un servidor activo basado en Opensource, para organizar, controlar y administrar de forma centralizada el acceso a los recursos de la red, y desarrollo: de los procedimientos y de las políticas para su administración, levantamiento de las políticas y manuales de administración aplicables a las particularidades de las direcciones que conforman la comandancia general del ejército"** fue realizado por los señores **Moncayo Sinchiguano, Flavio Rolando** y **Sánchez Changoluisa, Oscar Marcelo**, lo cual ha sido revisada y analizada en su totalidad por la herramienta de verificación de similitud de contenido; por lo tanto cumple con los requisitos legales, teóricos, científicos, técnicos y metodológicos establecidos por la Universidad de las Fuerzas Armadas ESPE, razón por la cual me permito acreditar y autorizar para que lo sustente públicamente.

Latacunga, 07 de marzo del 2022

VERONICA PAULINA TINTIN PERDOMO

Digitally signed by VERONICA PAULINA TINTIN PERDOMO
Date: 2022.03.05 18:45:19 -05'00'

Ing. Tintín Perdomo Verónica Paulina

C.C. 180292839-8

REPORTE DE VERIFICACIÓN DE CONTENIDO

COPYLEAKS

MONCAYO_SANCHEZ-TESIS FINAL.pdf

Scanned on: 0:5 March 6, 2022 UTC

Identical Words	935
Words with Minor Changes	217
Paraphrased Words	310
Omitted Words	0

COPYLEAKS Website | Education | Businesses

VERONICA PAULINA TINTIN PERDOMO

Digitally signed by VERONICA PAULINA TINTIN PERDOMO
Date: 2022.03.05 18:45:19 -05'00'

Ing. Tintín Perdomo Verónica Paulina

DIRECTORA

DEPARTAMENTO DE ELÉCTRICA Y ELECTRÓNICA

CARRERA DE TECNOLOGÍA SUPERIOR EN REDES Y TELECOMUNICACIONES

RESPONSABILIDAD DE AUTORÍA

Nosotros, **Moncayo Sinchiguano, Flavio Rolando** con cédula de ciudadanía Nº 050325292-6 y **Sánchez Changoluisa, Oscar Marcelo** con cédula de ciudadanía Nº 050324745-4, declaramos que el contenido, ideas y criterios de la monografía: "**Implementación de un controlador de dominio en la Comandancia General del Ejercito mediante un servidor activo basado en Opensource, para organizar, controlar y administrar de forma centralizada el acceso a los recursos de la red, y desarrollo: de los procedimientos y de las políticas para su administración, levantamiento de las políticas y manuales de administración aplicables a las particularidades de las direcciones que conforman la comandancia general del ejército",** es de nuestra autoría y responsabilidad, cumpliendo con los requisitos legales, teóricos, científicos, técnicos y metodológicos establecidos por la Universidad de las Fuerzas Armadas ESPE, respetando los derechos intelectuales de terceros y referenciando las citas bibliográficas.

Latacunga, 07 de marzo del 2022

FLAVIO ROLANDO MONCAYO SINCHIGUANO
Firmado digitalmente por FLAVIO ROLANDO MONCAYO SINCHIGUANO
Fecha: 2022.03.05 22:46:30 -05'00'

OSCAR MARCELO SANCHEZ CHANGOLUISA
Firmado digitalmente por OSCAR MARCELO SANCHEZ CHANGOLUISA
Fecha: 2022.03.05 22:53:12 -05'00'

Moncayo Sinchiguano, Flavio Rolando
C.C.: 050325292-6

Sánchez Changoluisa, Oscar Marcelo
C.C.: 050324745-4

DEPARTAMENTO DE ELÉCTRICA Y ELECTRÓNICA

CARRERA DE TECNOLOGÍA SUPERIOR EN REDES Y TELECOMUNICACIONES

AUTORIZACIÓN DE PUBLICACIÓN

Nosotros, **Moncayo Sinchiguano, Flavio Rolando** con cédula de ciudadanía Nº 050325292-6 y **Sánchez Changoluisa, Oscar Marcelo** con cédula de ciudadanía Nº 050324745-4 autorizamos a la Universidad de las Fuerzas Armadas ESPE publicar la monografía: "**Implementación de un controlador de dominio en la Comandancia General del Ejercito mediante un servidor activo basado en Opensource, para organizar, controlar y administrar de forma centralizada el acceso a los recursos de la red, y desarrollo: de los procedimientos y de las políticas para su administración, levantamiento de las políticas y manuales de administración aplicables a las particularidades de las direcciones que conforman la comandancia general del ejército",** en el Repositorio Institucional, cuyo contenido, ideas y criterios son de nuestra responsabilidad.

Latacunga, 07 de marzo del 2022

FLAVIO ROLANDO MONCAYO SINCHIGUANO
Firmado digitalmente por FLAVIO ROLANDO MONCAYO SINCHIGUANO
Fecha: 2022.03.05 22:46:30 -05'00'

Moncayo Sinchiguano, Flavio Rolando
C.C.: 050325292-6

OSCAR MARCELO SANCHEZ CHANGOLUISA
Firmado digitalmente por OSCAR MARCELO SANCHEZ CHANGOLUISA
Fecha: 2022.03.05 22:53:12 -05'00'

Sánchez Changoluisa, Oscar Marcelo
C.C.: 050324745-4

DEDICATORIA

El presente trabajo de titulación en primer lugar lo dedico a Dios porque es quien me ha regalado la vida, ha sido mi guía, fuerza y fortaleza para seguir y no parar ante ninguna de las adversidades que se han presentado en el transcurso de este tiempo.

A mis padres, quienes son el pilar fundamental de mi vida son aquellos que están de manera incondicional junto a mí en cada uno de los momento buenos o malos que he venido atravesando, aquellos que con sabiduría me han enseñado que nada en la vida es fácil que todo requiere de sacrificio, pero que si soy constante y perseverante todo lo que me proponga lo voy a lograr.

A mis hermanos, porque son el motivo de lucha diaria quienes que me han acompañado en el transcurso de este largo camino, me han bridado fuerza para seguir y han visto en mi el motivo de su inspiración para que un futuro ellos alcancen cada una de las metas y objetivos que se han planteado.

Y a cada una de las personas especiales que han llegado en el transcurso de mi vida, gracias por cada palabra de aliento por el apoyo incondicional y desinteresado que me han brindado y por enseñarme que el camino será muy duro en ciertas ocasiones pero que nada será imposible y lo voy a lograr; demostrando así que no se necesita tener lazos de sangre sino lazos de corazón.

Moncayo Sinchiguano, Flavio Rolando

AGRADECIMIENTO

A Dios Todopoderoso, porque cada mañana me da la dicha de poder abrir los ojos y saber que empieza un nuevo día lleno de muchas emociones y experiencias que me van formando en el ámbito personal y profesional.

A mis padres por todo el esfuerzo que han realizado para que pueda cumplir mi meta, por todo ese arduo trabajo que realizan día a día por darme un futuro mejor, a cada uno de sus consejos y enseñanzas que me han permitido levantarme de cualquier obstáculo que la vida me ponga.

A mi esposa y a mi hijo, por estar junto a mí en este largo camino por cada una de sus palabras por siempre confiar en mí y sobre todo por brindarme la seguridad de que lo iba a lograr, a mis hermanos, porque me han dado la fuerza y la motivación para luchar cada día.

A mi asesora de tesis, Ing. Verónica Tintín por su comprensión, apoyo y guía, por compartir cada uno de sus conocimientos y experiencias para poder culminar con éxito la meta planteada.

Por último, a la carrera de Tecnología Superior en Redes y Telecomunicaciones por haberme dado la oportunidad de prepararme profesionalmente, de enriquecer mi conocimiento y sobre todo darme una visión real de cómo es el ámbito profesional a futuro.

Sánchez Changoluisa, Oscar Marcelo

Tabla de contenido

Índice de figuras

Resumen

Las entidades e instituciones públicas actualmente, acarrean una gran problemática que surge en el uso de las mismas herramientas y dispositivos tecnológicos ya que existe personas mal intencionadas que intentan vulnerar la seguridad de la información altamente clasificada. Por ello, el objetivo general del presente proyecto de investigación se enfocó en la implementación del controlador de dominio cuyo objetivo es gestionar, administrar y resguardar los recursos de la red. Además, la metodología que se utilizó para la instalación del software de administración es el MSF, el cual permitió realizar la implementación de un controlador de dominio enfocado a los requerimientos de manera objetiva. En cambio, para el desarrollo se utilizó un software de código abierto (Open Sourse) Ubuntu Server 18.04 LTS que permitió establecer una mayor seguridad en la información, además se realizó la instalación de SSH para lograr una conexión remota y se instaló los servicios de Samba utilizando el protocolo Ldav, también se instaló el servicio remoto Windows6.1-Kb9588 que permitió gestionar las herramientas usuarios y equipos de Active Directory y la administración de directivas de grupo. Obteniendo así, la implementación de un controlador de dominio con la funcionalidad de un Active Directory que permita crear unidades organizativas, usuarios y establecer políticas de usuarios y equipos dentro cada uno de los departamentos de la CGFT e ingresarlos cada uno al dominio. Finalmente, con la administración del controlador de dominio se logró establecer las directrices para el uso de los equipos dentro de toda la unidad organizativa, teniendo en cuenta que se enfocó en los requerimientos e importancia de cada departamento.

Palabras claves:

- CONTROLADOR DE DOMINIO
- DIRECTORIO ACTIVO
- UBUNTU SERVER

Abstract

The public entities and institutions currently carry a great problem that arises in the use of the same tools and technological devices as there are malicious people who try to violate the security of highly classified information. Therefore, the general objective of this research project focused on the implementation of the domain controller whose objective is to manage, administer and safeguard the network resources. In addition, the methodology used for the installation of the management software is the MSF, which allowed the implementation of a domain controller focused on the requirements in an objective manner. On the other hand, for the development an Open-Source software (Open Sourse) Ubuntu Server 18.04 LTS was used, which allowed to establish a greater security in the information, in addition the installation of SSH was made to achieve a remote connection and the Samba services were installed using the Ldav protocol, also the Windows6.1-Kb9588 remote service was installed, which allowed to manage the Active Directory users and equipment tools and the administration of group policies. Thus, obtaining the implementation of a domain controller with the functionality of an Active Directory that allows to create organizational units, users and establish user and equipment policies within each of the departments of the CGFT and enter each of them to the domain. Finally, with the administration of the domain controller it was possible to establish guidelines for the use of equipment within the entire organizational unit, taking into account that it focused on the requirements and importance of each department.

Keywords:

- DOMAIN CONTROLLER
- ACTIVE DIRECTORY
- UBUNTU SERVER

Capítulo I

1. El Problema

1.1. Antecedentes

Actualmente desde que Microsoft hace el lanzamiento del sistema operativo Ubuntu Server 18.04, las organizaciones e instituciones empiezan a utilizar esta herramienta para gestionar roles y responsabilidades en la red, cuyo objetivo es asignar permisos, usuarios y grupos con el fin de administrar las políticas de la organización. Además, trae consigo el servicio de Directorio Activo, el cual almacena información de los recursos del dominio y permite el acceso controlado de usuarios y aplicaciones del servidor. Por ello la implementación de un controlador de dominio permite gestionar los privilegios sobre cada recurso (Ayovi, 2021).

Según Suárez Varela (2019), en el trabajo de investigación: “Implementación de un sistema de prevención de perdida de datos, con políticas de seguridad, mediante el control de dominio por medio de una herramienta de terceros”, desarrollado en la Cooperativa de Colombia con sede en Villavicencio, el objetivo fue establecer políticas de seguridad, para el cual fue necesario la participación de un grupo de estudiantes del seminario en seguridad informática y redes en entorno Microsoft; se realizó la implementación de la herramienta Device Lock DL y se obtuvo como resultado garantizar la disponibilidad, integridad, confidencialidad y buen uso de la información, concluyendo que con la correcta ejecución y la aplicación de las reglas en la herramienta Device Lock DLP se disminuyó la fuga de información.

Según Robayo Solano (2018) en el trabajo investigación: “Instalación y configuración del Zentyal Server 5.1 servicios como DNS, DHCP, Controladores de dominio, Cortafuegos, Proxy no Transparente y VPN”, desarrollado en la Universidad Nacional Abierta y a Distancia UNAD, el objetivo fue dar solución a diferentes problemas de migración e infraestructura en tecnologías de información, enfocados en

situaciones más complejas a niveles internos o externos de la red, en la cual participaron PYMES; mediante la instalación del servidor Zentyal en su versión 5.0, se obtuvo como resultado la implementación de servicios como DNS, DHCP, Controladores de dominio, Firewall, Proxy no Transparente y VPN como solución a un entorno profesional de networking y se concluyó que el acceso al Dominio creado en Zentyal server, requiere de una configuración previa del sistema operativo Ubuntu.

Según Borrero Núñez (2017), con el trabajo de investigación: “Active Directory (directorio activo) sistema de seguridad, control y privacidad de la información en la Gobernación del Tolima”, desarrollado en la Gobernación de Tolima con el objetivo Implementar el Servicio de Directorio Activo (Active Directory), el objetivo fue mejorar la seguridad y administración de los recursos tecnológicos, en el cual participaron 13 secretarías; mediante el Active Directory, se obtuvo como resultado el control y realizando el seguimiento al uso de los equipos tecnológicos al interior de la organización, de igual manera posibilita la generación de políticas de seguridad de la información y se concluyó la implementación de Active Directory como controlador de domino ayuda a las empresas e instituciones, a centralizar la seguridad y administración de los usuario y equipos tecnológicos, mejorando el nivel de seguridad ya que cada usuario debe identificarse para acceder a la red.

Por todo lo anteriormente expuesto acerca de la implementación de un controlador de dominio, se concluye que el objetivo principal es gestionar, administrar y controlar los recursos de una red, mediante la creación de una base de datos que contenga la información de los equipos informáticos conectados a la misma. Además, brindará seguridad y confiabilidad para los equipos mediante la autentificación de usuarios.

1.2. Planteamiento del problema

En la actualidad la Comandancia General de la Fuerza Terrestre mediante la Dirección de Tecnologías de Información y Comunicaciones, tiene como finalidad planificar, asesorar, ejecutar y supervisar el desarrollo, implantación e integración de los sistemas de información y comunicaciones, en concordancia con la planificación estratégica institucional, a través de personal altamente capacitado, manteniendo los principios éticos y morales de las fuerzas armadas, para contar con información oportuna y real que permita a los mandos en los diferentes niveles una adecuada toma de decisiones.

Por lo cual, dicha Institución maneja información altamente clasificada con respecto a futuras operaciones militares, teniendo en cuenta que el principal y más importante activo de una institución, empresa u organización está relacionada con dicha información, sin embargo, en la actualidad la más grande problemática surge en que de manera irónica con la utilización de las mismas herramientas y dispositivos tecnológicos, existen personas mal intencionadas que intentan acceder a datos que celosamente se resguardan en la institución.

Teniendo en cuenta que en la Comandancia General de la Fuerza Terrestre (CGFT), la problemática principal actualmente es que los recursos de red y sus departamentos no disponen de un software que ayude a gestionar, administrar y controlar los mismos, sobre todo que eviten que la información que se maneja sea expuesta de manera vulnerable a ataques informáticos, es necesario dar solución a la problemática.

Para ello, una vez identificado el problema se establece que la institución requiere crear un Active Directory que permita controlar y hacer un seguimiento al uso de los equipos tecnológicos al interior de la misma, de igual manera posibilita la generación de políticas de seguridad de la información con la finalidad de evitar el riesgo en el uso de

los dispositivos tecnológicos y el manejo de información sensible en cada una de las áreas de trabajo o despachos.

1.3. Justificación

El presente trabajo tiene la finalidad de gestionar los recursos de red mediante el uso de un directorio activo basado en OPEN SOURSE, que permitirá organizar, controlar y administrar de forma centralizada el acceso a los recursos de red, en la Comandancia General de la Fuerza Terrestre (CGFT), en la actualidad los recursos de red de la CGTF, y sus departamentos no disponen de un software que ayude a gestionar dichos recursos de red, convirtiéndose estos vulnerables para ataques informáticos.

La importancia de implementar un controlador de dominio dentro de la CGTF, es que se permitirá tener una base de datos con la información de los equipos informáticos conectados a la red y su administración en inventario, ayudará en la seguridad y confiabilidad de los equipos mediante la autentificación de sus usuarios, permitiendo gestionar los recursos de la red desde un solo servidor, estableciendo y aplicando políticas aplicables a la administración del servicio en las condiciones particulares de cada una de las direcciones.

Existe la factibilidad de realizar la investigación e implementación, debido a que se cuenta con el auspicio de la Dirección de Tecnologías de las información y comunicaciones DTIC’s de la CGFT, para la implementación se cuenta con personal que tiene conocimiento en el área de sistemas operativos, redes, y seguridad de la información. Además, que existe el conocimiento adecuado y suficiente por parte de los investigadores con respecto al tema, el apoyo en los recursos bibliográficos y el soporte de ayuda fundamentalmente con docentes especializados en tema de estudio.

Los beneficiarios de esta investigación serán los departamentos de la CGFT, y sus dependientes directos e indirectos, ya que por medio de la implementación del controlador de dominio se podrá optimizar los recursos de red de forma centralizada.

1.4. Objetivos

1.4.1. Objetivo general

Implementación de un controlador de dominio en la Comandancia General del Ejercito mediante un servidor activo basado en Opensource, para organizar, controlar y administrar de forma centralizada el acceso a los recursos de la red, y desarrollo: de los procedimientos y de las políticas para su administración, levantamiento de las políticas y manuales de administración aplicables a las particularidades de las direcciones que conforman la comandancia general del ejército.

1.4.2. Objetivos específicos

- Identificar los recursos necesarios para establecer un controlador de dominio, mediante un servidor activo basado en Open Sourse.
- Crear un controlador de dominio para un Active Directory mediante Ubuntu Server 18.04 LTS.
- Realizar manuales de instalación y políticas del en el respectivo controlador de dominio.

1.5. Alcance

El presente trabajo de investigación tiene como propósito realizar la implementación de un controlador de dominio en la Comandancia General de la Fuerza Terrestre. Principalmente se inicia con la identificación de todos los recursos necesarios para una red, que permitan gestionar, controlar y administrar la información de forma segura, posteriormente se creará el Active Directory que se lo relaciona como una base de datos que almacenará información de los usuarios y equipos que pertenecen a cada uno de los departamentos, mediante la utilización de software

Ubuntu Server 18.04. Finalmente, para evidenciar el desarrollo de la investigación se realizará un manual de instalación en el cual se establecerán paso a paso las actividades a desarrollar y un manual de las políticas, el cual contenga aspectos que ayuden a controlar con mayor eficiencia la seguridad informática.

Capítulo II

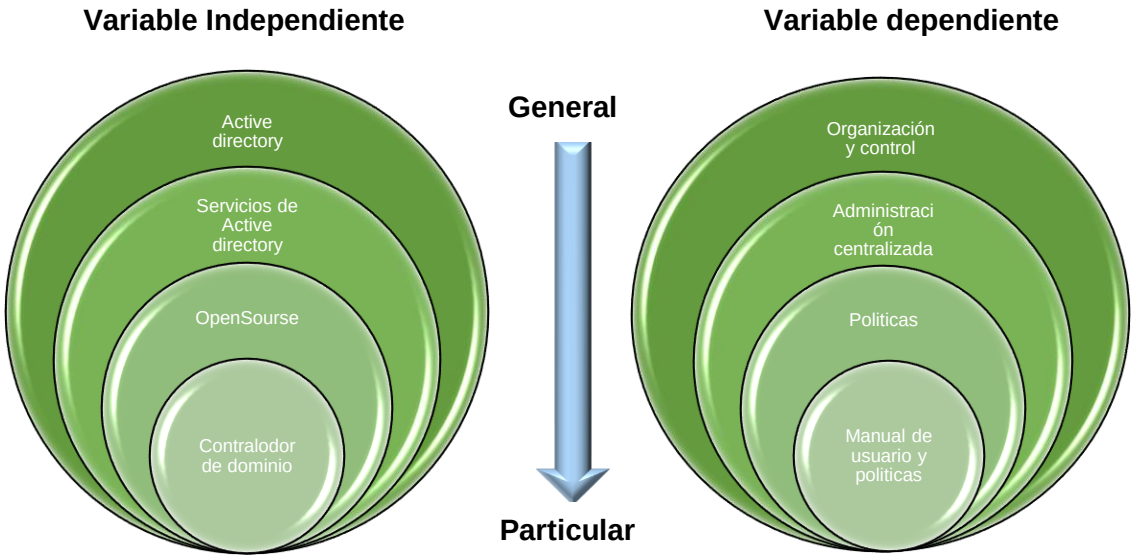
2. Marco teórico

2.1. Identificación de variables

Para la estructuración del marco teórico se ha tomado en cuenta la identificación de variables independientes y dependientes, mismas que serán fundamentadas mediante una investigación bibliográfica de cada uno de los temas encontrados dentro de las categorías teóricas.

Figura 1

Categorías Teóricas



2.2. Active Directory

Es una herramienta de Microsoft que proporciona servicios de directorio en una red, es capaz de ofrecer a cada usuario un servicio que puede estar ubicado en uno o más servidores de la empresa, administrar las credenciales de los diferentes usuarios, esta es la forma más sencilla de gestionar usuarios, bandejas de correo, documentos, bases de datos, tablas de Excel y mucho más (Gomar, 2019).

Además, es una estructura jerárquica que almacena información sobre los objetos de la red, proporciona los métodos para almacenar datos de directorio y hacer que estos datos estén disponibles para los usuarios y administradores, también permite que otros usuarios autorizados de la misma red tengan acceso a dicha información (Microsoft, 2021).

2.2.1. Requisitos de instalación

Según Simad (2017), establece que a la hora de crear un dominio se deben cumplir con determinados requisitos, que vamos a mencionar a continuación:

Se debe tener una unidad de disco formateada con más de 250 MB.

Hay que contar con alguna versión Server de Windows.

Instalar y configurar el protocolo TCP/IP.

Poseer un servidor de nombre DNS.

2.2.2. Ventajas

Según Tecnozero (2019), las ventajas que tiene el Directorio activo de Ubuntu Server 18.04 para una empresa, institución u organización son las que se menciona a continuación:

Organización: permite crear grupos para facilitar la administración.

Permisos: es el control desde un sólo punto de los permisos a los recursos de la red.

Autenticación: cualquier usuario puede entrar en otro equipo de la red con su usuario y clave y tendrá los permisos que le hayamos asignado.

Políticas: puedes controlar el comportamiento de los equipos y permisos de los usuarios de forma muy concreta.

Escalabilidad: es un sistema que funciona en un solo servidor y tres usuarios y para miles de usuarios repartidos por varias sedes y varios servidores repartiendo la carga.

Autenticación externa: permite que otras aplicaciones lean los datos.

Replicación: implementa características para la replicación de todos los datos entre servidores del directorio activo

2.2.3. Desventajas

Sin embargo, Dell (2018) establece las desventajas respectivas que se pueden ocasionar dentro del Directorio activo de Ubunto Server 18.04, las cuales se menciona a continuación:

- Si se quitan usuarios del grupo de Active Directory, las cuentas permanecerán en el grupo de PS Series, reduciendo la cantidad máxima de cuentas de usuario.
- El administrador de grupos debe quitar manualmente las cuentas de Active Directory sin uso.
- El uso de Active Directory ofrece mayor nivel de escalabilidad con el uso de cuentas locales.
- Si existen cambios frecuentes en la lista de cuentas, el administrador de grupos debe hacer actualizaciones frecuentes.

2.2.4. Servicios

Según Paessler (2018), menciona que con el tiempo Microsoft ha agregado servicios adicionales como se detallan a continuación bajo el estándar de Active Directory:

Active Directory Lightweight Directory Services: elimina cierta complejidad y algunas características avanzadas para ofrecer solo la funcionalidad básica del servicio de directorio sin controladores de dominio o bosques.

Active Directory Certificate Services: este servicio puede almacenar, validar, crear y revocar las credenciales de clave pública utilizadas para el cifrado en lugar de generar claves de forma externa o local.

Active Directory Federation Services: proporciona un servicio de autenticación y autorización de inicio de sesión único basado en la web para su uso principalmente entre organizaciones.

Active Directory Rights Management Services: se trata de un servicio de administración de derechos que rompe con el concepto de autorización como un simple modelo de permitir o denegar acceso.

2.3. Open Sourse

También conocida como fuente abierta hace referencia a todos aquellos programas informáticos que disponen a cualquier usuario el acceso a su código de programación facilitando por parte de otros programadores ajenos la modificación del mismo. No debemos confundir en ningún momento con Software Libre que es software que puede descargarse y distribuirse de manera gratuita (Openexpoeurope, 2021).

2.3.1. Valores

Según Redhat (2019), hay muchas razones por las que las personas eligen el software open source en lugar del software propietario, pero las más conocidas son las que se mencionan a continuación:

Revisión entre compañeros: puede acceder al código fuente libremente los colegas programadores verifican y mejoran el open source.

Transparencia: puede verificar la información y realizar un seguimiento, sin tener que depender de las promesas de los proveedores.

Confiabilidad: el código propietario depende de un solo autor o una sola empresa que lo controlan para mantenerlo actualizado, con parches y en funcionamiento.

Flexibilidad: puede utilizarlo para abordar los problemas específicos de su empresa o comunidad, implementando soluciones nuevas.

Menor costo: con el open source, el código en sí es gratuito.

Sin dependencia de un solo proveedor: puede trasladar el open source a cualquier parte y usarlo para lo que sea en cualquier momento.

Colaboración abierta: brindan la posibilidad de buscar ayuda, recursos y puntos de vista que trascienden el interés de un grupo o una empresa.

2.4. Controladores de dominio

Según Ediciones-eni (2018), el controlador de dominio es un servidor que ejecuta el sistema operativo Windows Server en el que un administrador ha implementado el servicio de dominio a través de Active Directory, estos pueden ser de dos tipos:

Controladores de dominio (en escritura)

Controladores de dominio de solo lectura.

Además, Msinetworks (2020) establece que un controlador de dominio se relaciona con una red que aloja varias computadoras y dispositivos, el mismo que se lo toma en cuenta como un concentrador maestro al que están conectados todos los dispositivos y puede controlar cualquier dispositivo que sea parte de la red; por ello incluyen los siguientes equipos e instrumentos que son:

- Ordenadores
- Laptops
- Cámaras de seguridad
- Servidores

2.4.1. Beneficios

Según Msinetworks (2020), menciona que los controladores de dominio eliminan las conjeturas y las molestias de administrar computadoras y dispositivos en su red al "conectarlos" a un sistema maestro, lo cual le permite a su administrador establecer salvaguardas, permisos y otros protocolos de acceso de forma remota en cada dispositivo. Por ello se establecen las siguientes razones que se menciona a continuación al conectar la red a un controlador de dominio:

- Dar acceso solo aquellos que lo necesitan.
- Evite las infracciones de datos de "error del operador"
- La gestión centralizada reduce los costos
- Recursos informáticos compartidos
- Administre fácilmente las impresoras de red

2.4.2. Características

Según Birtlh (2020) para llegar al momento en que el servicio de directorio se comporte para lo que fue diseñado, debemos seguir un proceso de instalación, configuración y personalización; sin embargo, antes de implementar un directorio hay que hacer una planificación anticipada de ciertos aspectos que se mencionan a continuación:

- Definir para qué se utilizará, es decir, definir los contenidos del directorio.
- Decidir cuál será la organización de los datos antes de comenzar.
- Pensar qué forma tendrá este árbol de información del directorio o DIT.

2.5. Estructura y control de un Active Directory

Según Tecnozero (2019), la estructura y control de un directorio activo se encuentra compuesta por los siguientes objetos que se menciona a continuación:

Recursos: como impresoras, equipos, etc.

Servicios: como correo, Web, FTP, etc.

Usuarios: y toda la información necesaria de los mismos, incluyen cuentas para conectarse, grupos de trabajo, etc.

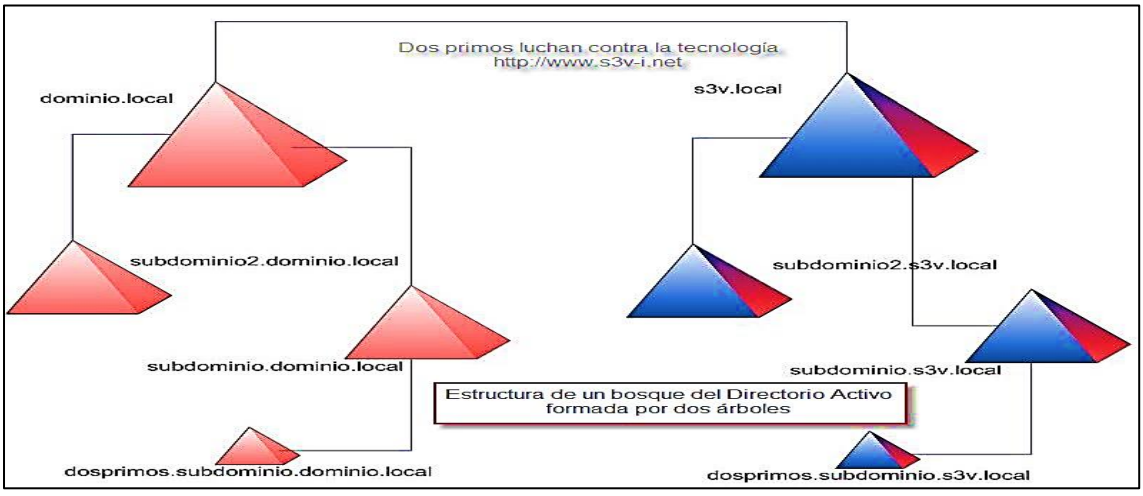
2.6. Tipos de control de un Active Directory

2.6.1. Bosque

Es el nivel más alto de la jerarquía y se trata de un límite de seguridad dentro de la organización, además permite segregar la delegación de autoridad de forma acotada en un solo entorno. De este modo, podemos tener un administrador con derechos y permisos de acceso total, pero solo a un subconjunto específico de recursos. También es posible utilizar un solo bosque en la red, la información se almacena en todos los controladores de dominio de todos los dominios dentro del bosque (Paessler, 2018).

Figura 2

Estructura de tipo bosque



Nota. Tomado de *(Martinez, 2008)*

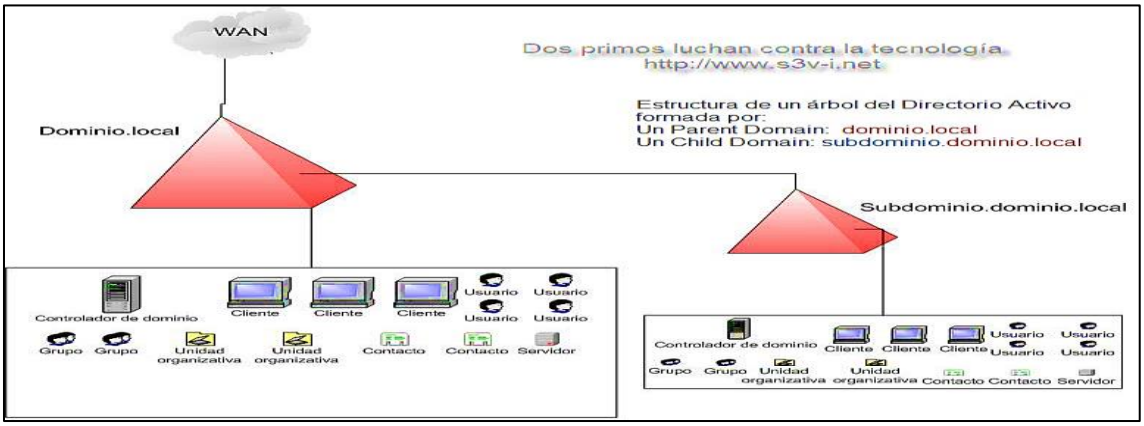
2.6.2. Árbol

Es un grupo de dominios que dentro de un árbol comparten el mismo espacio de nombre raíz, pero, a pesar de ello no son límites de seguridad o replicación. (Paessler, 2018)

El objetivo de crear este tipo de estructura es fragmentar los datos del Directorio Activo, replicando sólo las partes necesarias y ahorrando ancho de banda en la red. (Ruiz, 2013)

Figura 3

Estructura de tipo árbol



Nota. Tomado de *(Martinez, 2008)*

2.6.3. Unidades organizativas (OU)

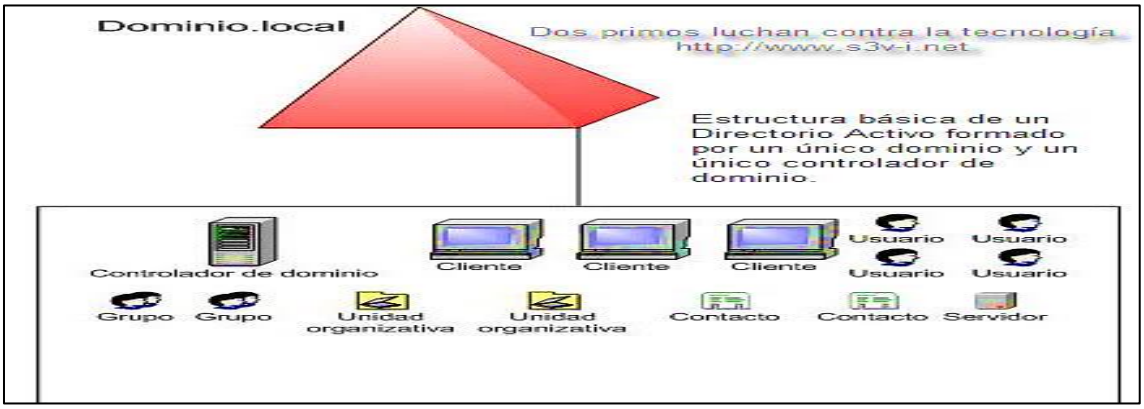
Permite agrupar la autoridad sobre un subconjunto de recursos de un dominio, además proporciona un límite de seguridad para privilegios y autorización elevados, pero no limita la replicación de objetos de AD. También, se utilizan para delegar el control dentro de agrupaciones funcionales, se usan para implementar y limitar la seguridad y los roles entre los grupos, mientras que los dominios deben usarse para controlar la replicación de Active Directory (Paessler, 2018).

2.6.4. Dominios

Cada bosque contiene un dominio raíz y se pueden usar dominios adicionales para crear más particiones dentro de un bosque, el propósito es dividir el directorio en partes más pequeñas para poder controlar la replicación, además limita la replicación de Active Directory solo a los otros controladores de dominio que se encuentran en su interior y cada controlador contiene una copia idéntica de la base de datos de Active Directory, de este modo se mantiene todo actualizado a través de la replicación constante. Se recomienda que no sean solo los dominios los que se encarguen de controlar la replicación, sino que se empleen también las unidades organizativas para agrupar y limitar los permisos de seguridad (Paessler, 2018).

Figura 4

Estructura de tipo dominio



Nota. Tomado de *(Martinez, 2008)*

2.7. Metodología Microsoft® Solutions Framework

Es un marco de trabajo de referencia para construir e implantar sistemas empresariales distribuidos basados en herramientas y tecnologías de Microsoft MSF, comprende un conjunto de modelos, conceptos y guías que contribuyen a alinear los objetivos de negocio y tecnológicos, reducir los costos de la utilización de nuevas tecnologías, y asegurar el éxito en la implantación de las tecnologías Microsoft. (Sites.google, 2014)

2.8. Fases de la metodología MSF

Según la página Google Sites (2014), con respecto a las fases de la metodología menciona que:

Visión

Es aquella donde el equipo y el cliente definen los requerimientos del negocio y los objetivos generales del proyecto, la cual culmina con el hito visión y alcance aprobados.

Planeación

Durante esta fase de planeación el equipo crea un borrador del plan maestro del proyecto, además de un cronograma del proyecto y de la especificación funcional del proyecto, la cual culmina con el hito plan del proyecto aprobado. Se levantarán los requerimientos específicos del cliente, es decir que permite cambios dentro del proyecto, incluso en la etapa de desarrollo

Desarrollo

Esta fase involucra una serie de requerimientos internos del producto, desarrollados por partes para medir su progreso y asegurarse que todos sus módulos o partes están sincronizados, pueden integrarse y culmina con el hito alcance completo. Propiamente se genera el código necesario para un producto funcional para el cliente.

Estabilización

Esta fase se centra en probar el producto y proceso de prueba hace énfasis en el uso y el funcionamiento del producto en las condiciones del ambiente.

Implementación

En esta fase el equipo implanta la tecnología y los componentes utilizados por la solución, estabiliza la implantación, apoya el funcionamiento y la transición del proyecto, y obtiene la aprobación final del cliente. La fase termina con el hito implementación completa

2.9. Políticas

Es una función de Windows que le permite controlar las operaciones de cuentas, aplicaciones y el propio Windows, está destinado principalmente para uso empresarial, en donde se podrá realizar las GPO significa Objeto de política de grupo, la misma que se refiere a una colección de configuraciones de políticas de grupo definidas para un sistema específico, cuando alguien inicia sesión en una computadora del dominio, esa máquina se registra con el controlador de dominio y se apodera de cualquier cambio reciente de la Política de grupo (Ephesos Software, 2019).

2.10. Configuraciones

Según Reparar.info (2021), se debe considerar las seis configuraciones de Windows disponibles que se mencionan a continuación para las contraseñas en GPO:

Cumplir el historial de contraseñas: es aquel que determina el número de contraseñas antiguas almacenadas.

Antigüedad máxima de la contraseña: establece la caducidad de la contraseña en días.

Longitud mínima de la contraseña: se recomienda que las contraseñas contengan al menos 8 símbolos

Antigüedad mínima de la contraseña: establece la frecuencia con la que los usuarios pueden cambiar sus contraseñas.

La clave debe cumplir los requerimientos de complejidad: si la política está habilitada, un usuario no puede usar el nombre de la cuenta en una contraseña, se deben usar 3 tipos de símbolos, letras mayúsculas, letras minúsculas y caracteres especiales.

Almacene las contraseñas mediante cifrado reversible: las contraseñas de los usuarios se almacenan cifradas en la base de datos.

2.11. Aplicaciones

Según Ranchal (2021), hay centenares de opciones, preferencias y configuraciones diferentes que se pueden activar, por ello un mal ajuste puede causar problemas o comportamientos no deseados. Sin embargo, hay controles sencillos que pueden ser útiles para redes locales o máquinas cliente y que nos sirven para empezar a conocer las posibilidades de este gestor. Como por ejemplo las siguientes aplicaciones que se mención a continuación:

Restringir el acceso al panel de control y configuración: son vitales para redes empresariales y entornos escolares, pero también pueden ser útiles en el hogar para computadoras compartidas entre múltiples usuarios.

Bloquear acceso al símbolo del sistema: es aquella que impide la ejecución del símbolo del sistema y también la ejecución de archivos por lotes en formatos CMD o BAT.

Impedir la instalación de software: es aquella que impide la introducción de malware o aplicaciones basura y permiten reducir de paso la carga y mantenimiento del sistema.

Deshabilitar reinicios forzados: es aquella que permite no reiniciar automáticamente con usuarios que hayan iniciado sesión en instalaciones de actualizaciones automáticas.

Deshabilitar las unidades extraíbles: es aquella que desactiva el acceso de lectura o escritura de medios ópticos, de los disquetes o de unidades de almacenamiento flash, aunque los USB persistentes siempre son los más problemáticos.

Ejecutar scripts en el inicio de sesión / inicio / apagado: es aquella que permite ejecutar scripts con los archivos por lotes que pueden escribirse en la consola PowerShell, se pueden activar automáticamente.

Desactivar las actualizaciones automáticas de controladores: es aquella que bloquea a los controladores sin permiso implícito del usuario que realicen actualizaciones automáticas de controladores.

2.12. Manuales

Es el documento que contiene la descripción de actividades que deben seguirse en la realización de las funciones de una unidad administrativa, o de dos o más de ellas, además incluyen los puestos o unidades administrativas que intervienen precisando su responsabilidad y participación (Scielo, 2017)

2.13. Tipos

Según Softgrade (2021), se puede clasificar a los manuales que utiliza una organización con base al objetivo que desean conseguir, dentro de las principales clasificaciones podemos encontrar las siguientes:

Manual de políticas

Es aquel donde se encuentran todas las políticas sobre las cuales se rige la operación de la organización, el cual permitirá normalizarse en todas las áreas.

Manual de usuario

Es aquel que contiene un conjunto de informaciones, instrucciones y advertencias relacionadas con el uso de un determinado producto o servicio.

2.13.1. Ventajas

Según Google Sites (2011), se establecen las ventajas respectivas que se debe tomar en cuenta para la elaboración y uso de los diferentes manuales, las cuales se detallan a continuación:

- Permiten al usuario tener una guía o tutorial que les va a permitir iniciar la creación de su página, paso a paso.
- Cualquiera puede acceder a crear su página.
- Fácil de usar y aprender.
- Personas situadas en diferentes partes del mundo pueden acceder trabajar en el mismo documento o manual.
- Amplía el acceso al poder de publicación web para usuarios no técnicos
- Es una herramienta flexible que puede utilizarse para una amplia gama de aplicaciones.
- Son herramientas sin costo.
- Permite tener una información secuencial.
- Permite dar a conocer diferentes programas para crear páginas Web.

2.13.2. Desventajas

Sin embargo, Google Sites (2011) establece las desventajas respectivas para la elaboración y uso de los diferentes manuales, las cuales se menciona a continuación:

- Algunas consideran que es demasiado caro, limitativo y laborioso preparar un manual y conservarlo al día.
- Existe el temor de que pueda conducir a una estricta reglamentación y rigidez.
- Su deficiente elaboración provoca serios inconvenientes en el desarrollo de las operaciones.
- El costo de producción y actualización puede ser alto.
- Si no se actualiza periódicamente, pierde efectividad.
- Incluye solo aspectos formales de la organización, dejando de lado los informales, cuya vigencia e importancia es notorio para la misma.
- Muy sintética carece de utilidad.

Capítulo III

3. Desarrollo del tema

3.1. Metodología

Con el propósito de cumplir con cada uno de los objetivos planteados para el desarrollo del presente proyecto, se considera conveniente aplicar los siguientes procedimientos de investigación:

3.1.1. Modalidad básica de investigación

Investigación Bibliográfica

En la presente investigación se utiliza información primaria proporcionada por parte de la Comandancia General de la Fuerza Terrestre y fuentes bibliográficas secundarias a través de libros, revistas, artículos científicos, tesis referentes a la problemática, entre otros; los mismos que son obtenidos mediante internet, evaluando la fundamentación teórica y criterios adecuados referentes a la implementación de un controlador de dominio, cuyo fin es proporcionar un desarrollo sustentable a la presente investigación.

Investigación de Campo

La modalidad utilizada para el desarrollo del presente proyecto será la investigación de campo en vista que se debe acudir a las instalaciones de la Comandancia General de la Fuerza Terrestre ubicada en la Provincia de Pichincha en la ciudad de Quito sector la Recoleta, para observar la condición actual del manejo de información clasificada de cada uno de los departamentos, en la cual se obtendrán datos importantes con respecto a la vulnerabilidad de la seguridad de la información digital en los mismos, por medio de observaciones, apuntes e imágenes que otorgan una información verídica de beneficio mutuo tanto para la Institución como para los investigadores.

Investigación Aplicada

Se considera esta modalidad de investigación ya que se orienta al desarrollo de la implementación de un controlador de dominio para organizar, controlar y administrar de forma centralizada el acceso a los recursos de la red dentro de la CGFT, mediante la aplicación del conocimiento adquirido durante los años de estudio y la investigación del método más adecuado para la implementación del mismo.

3.1.2. Nivel o tipo de investigación

Investigación Descriptiva

Es aquella que permite analizar, describir, documentar y mejorar los métodos que se utilizan dentro de la implementación del controlador de dominio, cuyo fin es organizar, controlar y administrar de forma centralizada el acceso a los recursos de red en la CGFT. Además, ayudará en la seguridad y confiabilidad de los equipos mediante la autentificación de los usuarios, permitiendo gestionar los recursos de la red desde un solo servidor.

3.1.3. Metodología Microsoft® Solutions Framework (MSF)

Es aquella que permite construir e implementar sistemas administrativos como un controlador de dominio o active directory basado en herramientas y tecnologías actuales, consta de 5 etapas principales que son: visión, planeación, desarrollo, estabilización e implementación las cuales se enfocan en resolver los requerimientos de un sistema administrativo de una manera objetiva.

3.2. Diseño e Implementación

3.2.1. Información general de la CGFT

Reseña Histórica

La historia del Ejército ecuatoriano va de la mano con la gesta imperecedera del 10 de agosto de 1809, cuando al albor de la libertad, nace el Ejército ecuatoriano, cuya

labor en más de dos siglos ha contribuido indiscutiblemente a la edificación del Ecuador democrático y soberano. (Ejercito Ecuatoriano, 2020)

Las ideas progresistas del quiteño Javier Eugenio de Santa Cruz y Espejo, del influjo del espíritu de la Revolución Francesa y de la independencia de los Estados Unidos, en la fecha épica del 10 de agosto de 1809, naciera no solo una nueva etapa para Quito y el continente, sino el inicio de lo que hoy conocemos como el Ejército ecuatoriano.

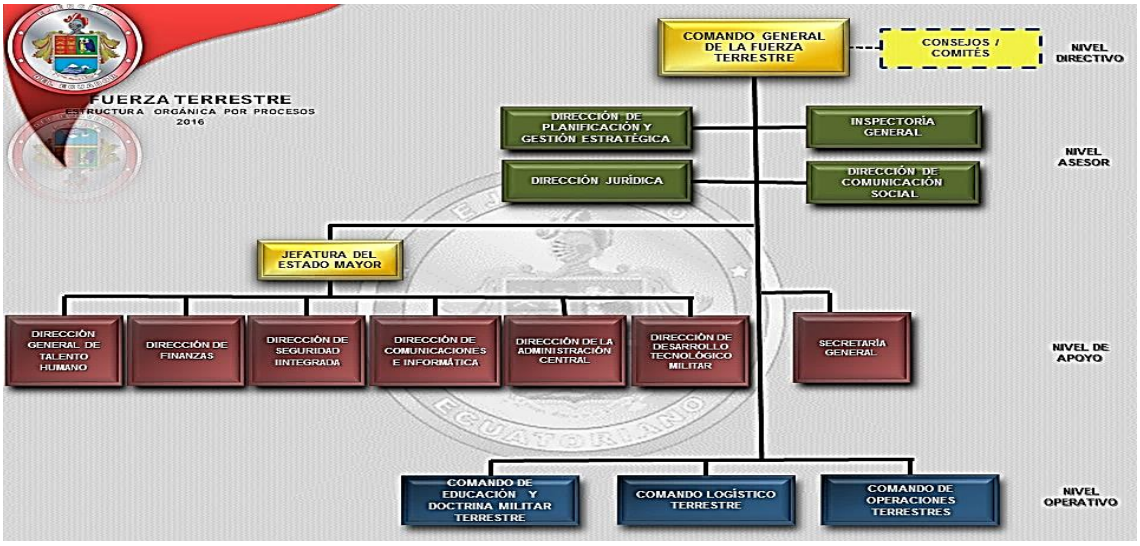
La formación del Ecuador como república en 1830 afirma la identidad del Ejército y lo formaliza como un ente con espíritu constitucional, cuando en Riobamba, el 11 de septiembre de 1830, al albor de la primera Carta Magna. (Ejercito Ecuatoriano, 2020)

3.2.2. Estructura Orgánica

La estructura orgánica que posee la CGFT es de tipo vertical, como se muestra en la *figura 5,* ya que consta de 4 niveles entre los cuales se tiene el directivo, asesor, de apoyo y el operativo.

Figura 5

Estructura Orgánica de la CGFT



Nota. Tomado de *(Ejercito Ecuatoriano, 2020)*

3.2.3. Misión

El Ejército Ecuatoriano desarrolla el poder militar terrestre, preparando, entrenando y equipando al personal militar profesional, para ejecutar las operaciones que coadyuven a la defensa de la soberanía e integridad territorial al desarrollo nacional y a la seguridad integral; en tiempos de paz, crisis o guerra hasta el cese de los mismos, mejorando las capacidades operativas en forma permanente a fin de ejecutar el control efectivo del espacio terrestre y promover la paz. (Ejercito Ecuatoriano, 2020)

3.2.4. Visión

Al 2033 ser un Ejército multimisión, con personal polivalente y medios multipropósito; promotor de principios y valores, comprometido con la sociedad, que contribuya a la integración y Desarrollo Nacional. (Ejercito Ecuatoriano, 2020)

3.3. Desarrollo de la propuesta

Para iniciar con el desarrollo de la Implementación de un controlador de dominio en la Comandancia General de la Fuerza Terrestre (CGFT), primero se debe realizar la instalación de Ubuntu Server 18.04 LTS, posteriormente la actualización de los paquetes, luego configurar la tarjeta de red, se continua con la instalación de SSH, luego la configuración de servidores DNS e instalación del servicio Samba, consecuentemente la activación del servicio automático del directorio activo como controlador de dominio, finalmente se debe realizar la instalación de la herramienta de administración remota y la activación correspondiente.

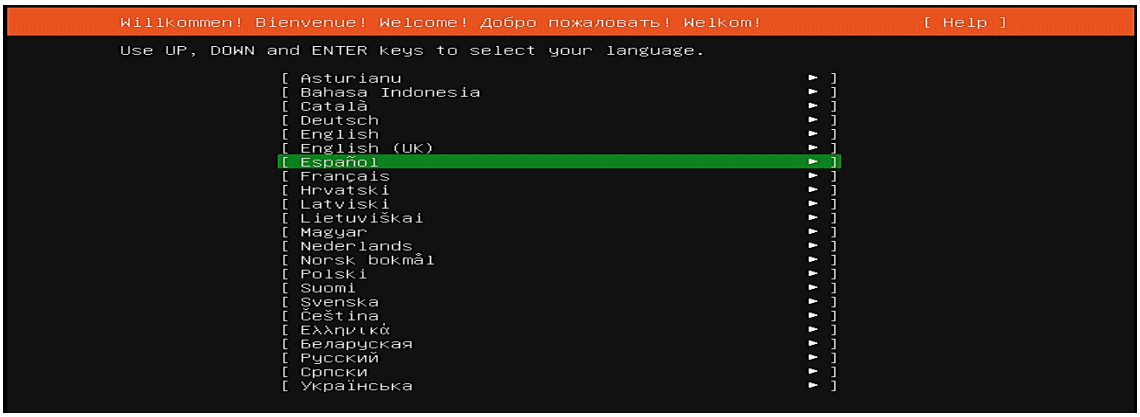
3.3.1. Instalación de Ubuntu Server 18.04 LTS

Para iniciar con el desarrollo de la propuesta fundamentalmente se requiere la instalación de Ubuntu Server 18.04 LTS, cuyo fin es complementar la ejecución del controlador de dominio en la CGFT, por ello se detalla la instalación del mismo a continuación.

Inicialmente se descarga el software de la página oficial de Ubuntu versión 18.04 LTS, posteriormente se ejecuta como administrador en el cual se despliega la pantalla select your language como se indica en la *figura 6***,** donde se selección el idioma de mejor comprensión que para este caso es el español.

Figura 6

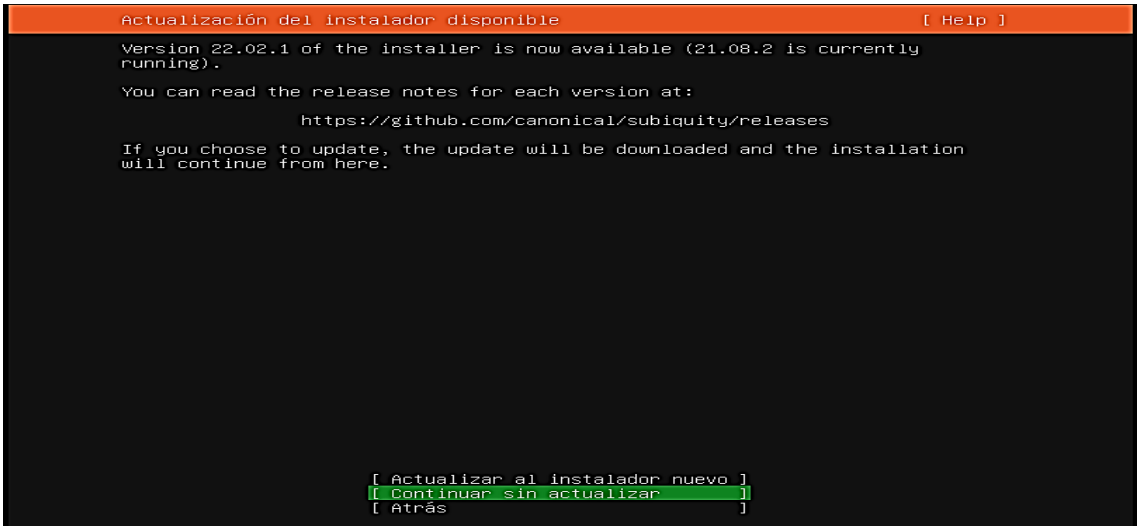
Selección del idioma



Luego se muestra la ventana actualización del instalador disponible como se muestra en la *figura 7*, en la cual por el momento se debe seleccionar continuar sin actualizar con el fin de evitar algún conflicto o error durante la instalación.

Figura 7

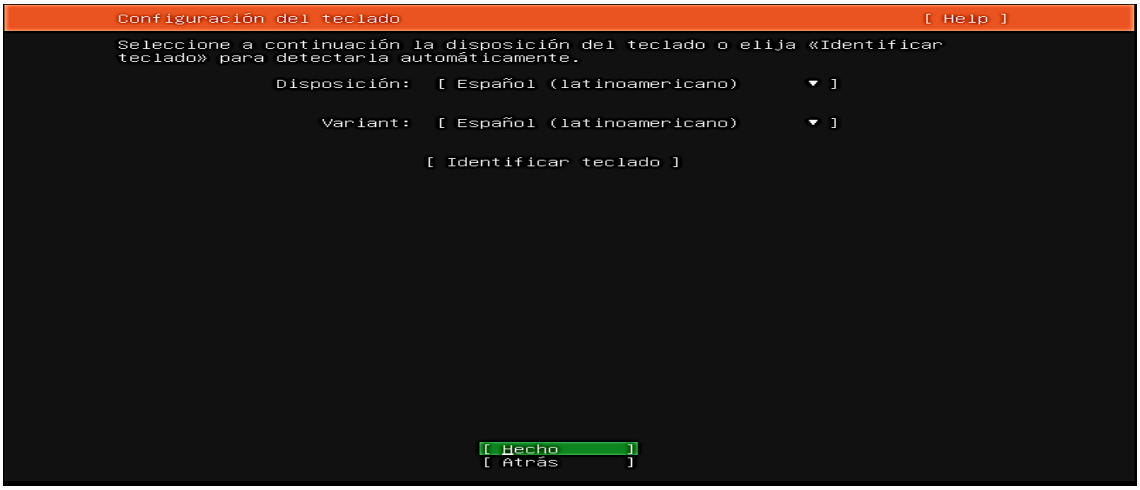
Actualización del instalador disponible



Posteriormente se despliega la ventana configuración del teclado como se muestra en la *Figura 8*, en el cual se debe elegir el idioma tomando en cuenta que es el español y no el latinoamericano y dar clic en hecho.

Figura 8

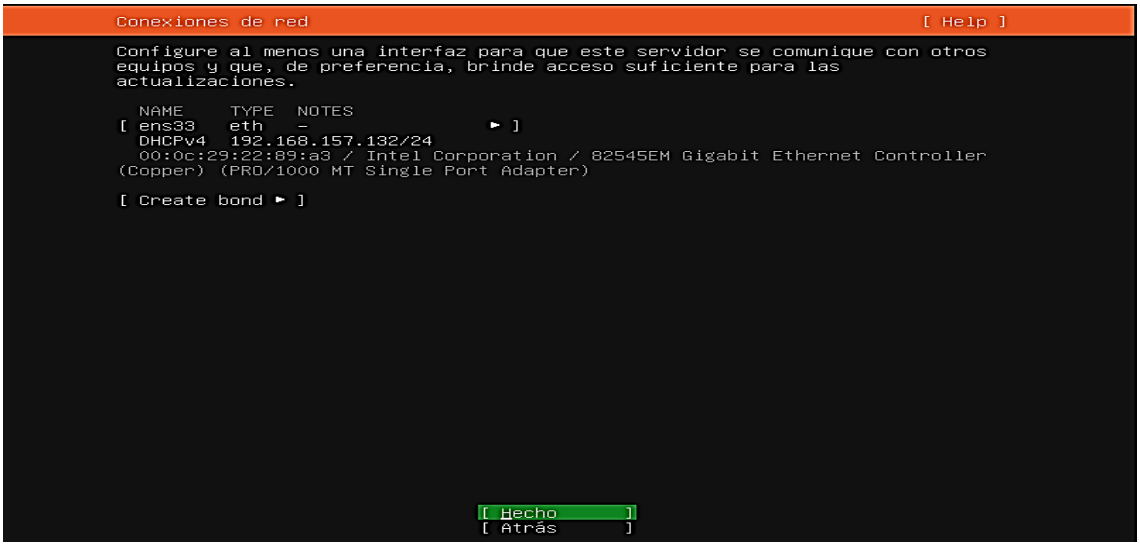
Configuración del teclado



Luego se muestra la ventana conexiones de red como se indica en la *figura 9*, en el cual se procede a dejar en automático la dirección IP, ya que después se realizará la configuración de la tarjeta de red y dar clic en hecho.

Figura 9

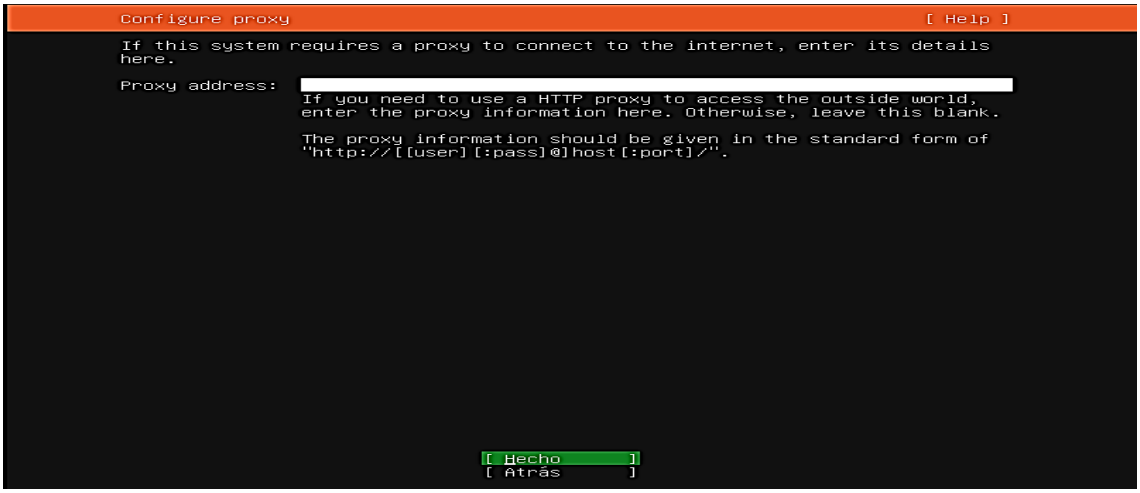
Conexiones de red



Posteriormente se despliega la ventana configuración de proxy como se indica en la *figura 10*, en la cual si se realiza la conexión a través de un Proxy en este casillero se procede a especificarlo o se puede dejar en blanco y dar clic en hecho.

Figura 10

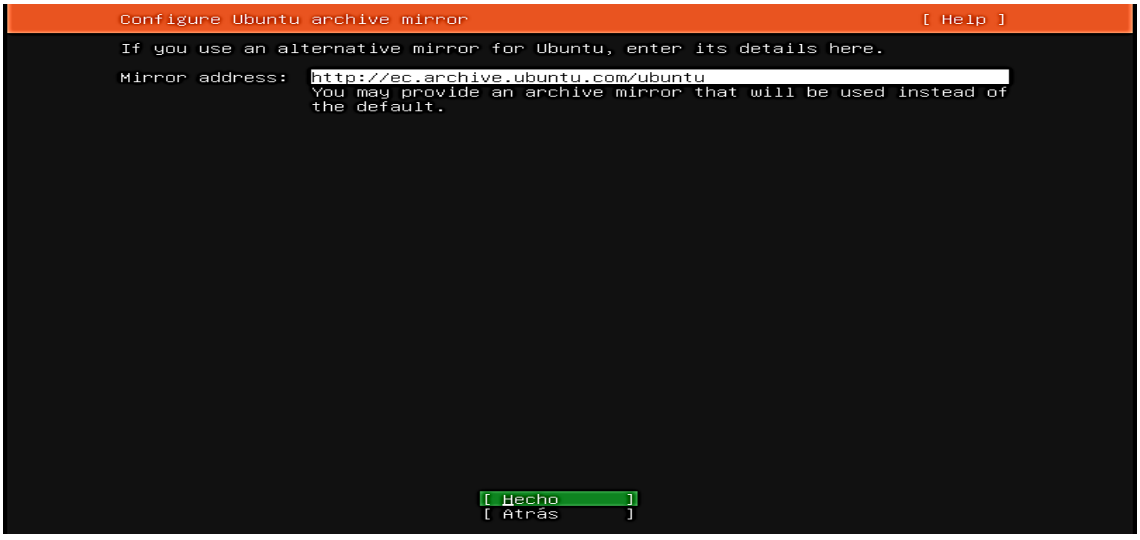
Configuración proxy



Luego se muestra la ventana configure Ubuntu archive mirror como se indica en la *figura 11*, en donde se procede a dar clic en hecho ya que no se utilizará una ventana alternativa para Ubuntu.

Figura 11

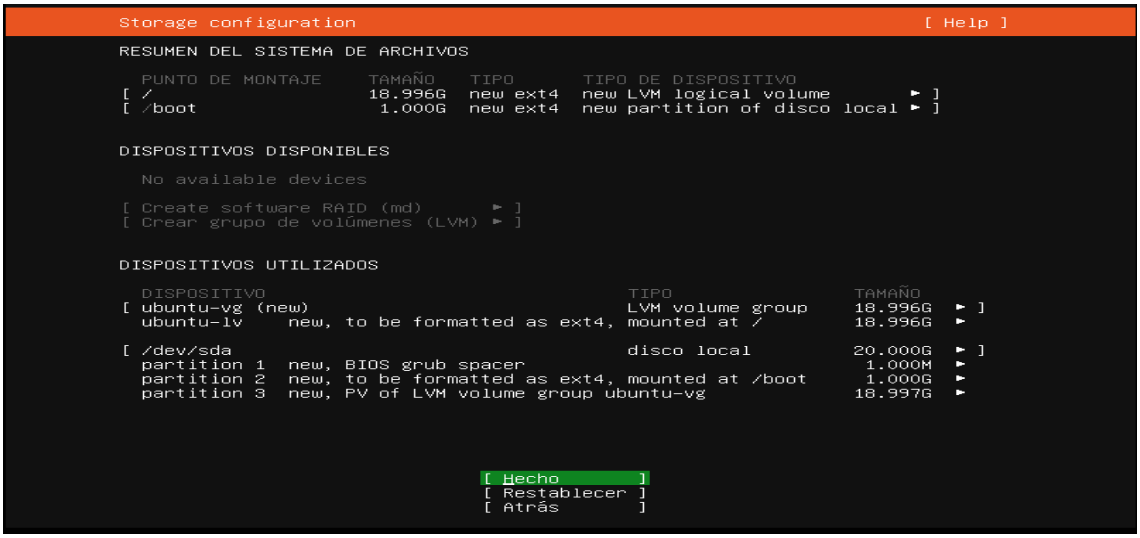
Ventana alternativa para Ubuntu



Posteriormente se despliega la ventana storage configuration como se indica en la *figura 12*, en el que se procede a elegir la unidad del disco rígido con sus diferentes particiones; en este caso se utiliza todo el disco y dar clic en hecho.

Figura 12

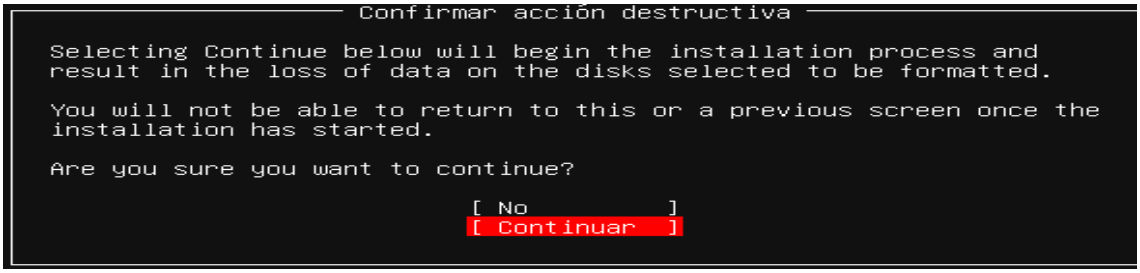
Configuración de almacenamiento



Luego se muestra la ventana confirmar acción destructiva como se indica en la *figura 13*, en esta parte sale una advertencia del disco rígido en donde se destruirá todos los archivos y luego dar clic en continuar.

Figura 13

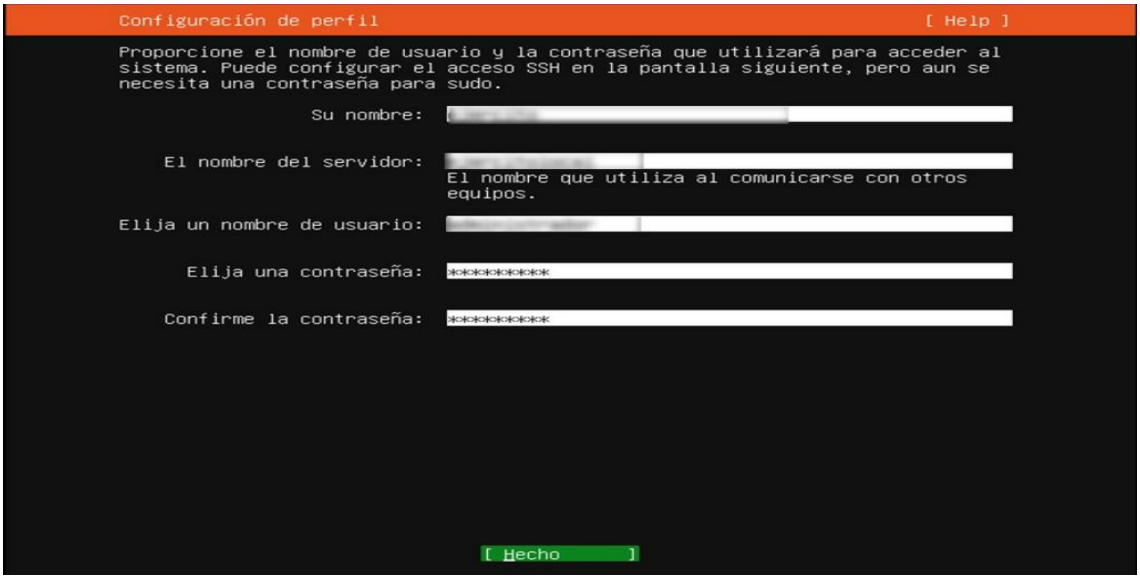
Confirmar acción destructiva



Posteriormente se despliega la ventana configuración del perfil como se indica en la ***Figura 14***, en el cual se detalla cada una de las características del servidor como el nombre tanto del servidor y como del usuario, contraseñas y luego dar clic en hecho.

Figura 14

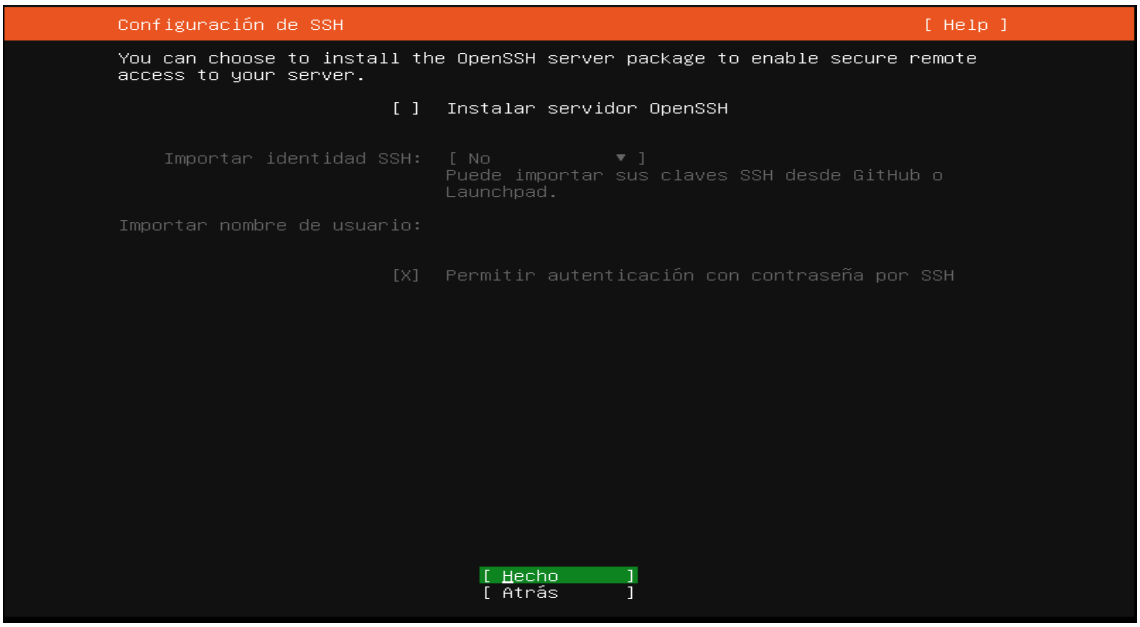
Configuración de perfil



Luego se muestra la ventana configuración de SSH como se indica en la *figura 15*, en donde se procede a dar clic en hecho ya que posteriormente se realizará la instalación del paquete SSH para una mejor configuración del controlador de dominio.

Figura 15

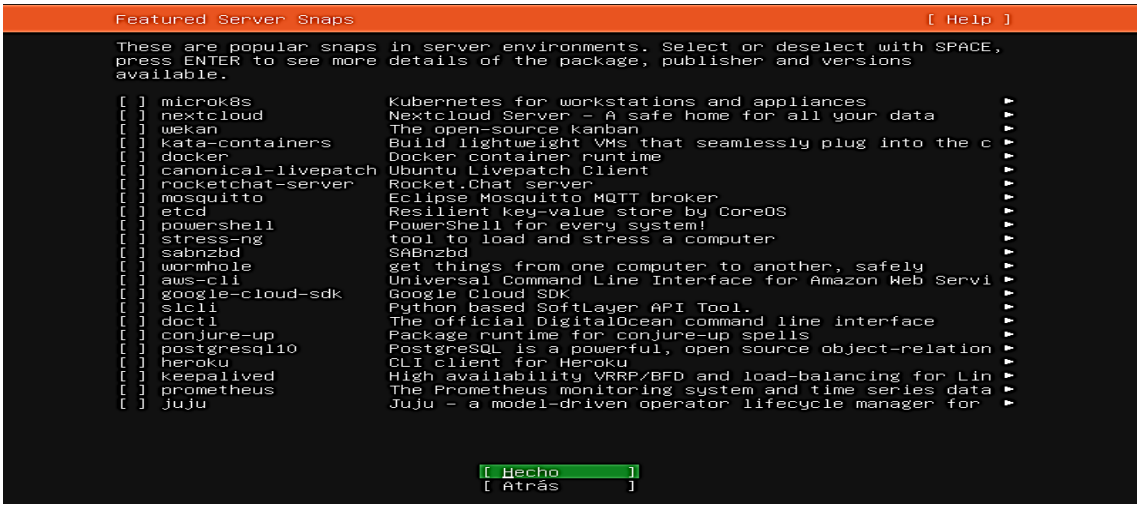
Configuración de SSH



Posteriormente se despliega la ventana featured server snaps como se indica en la *figura 16*, en donde se procede a realizar la instalación de Ubuntu Server y no se debe seleccionar ningún paquete ya que no son necesarios y luego dar clic en hecho.

Figura 16

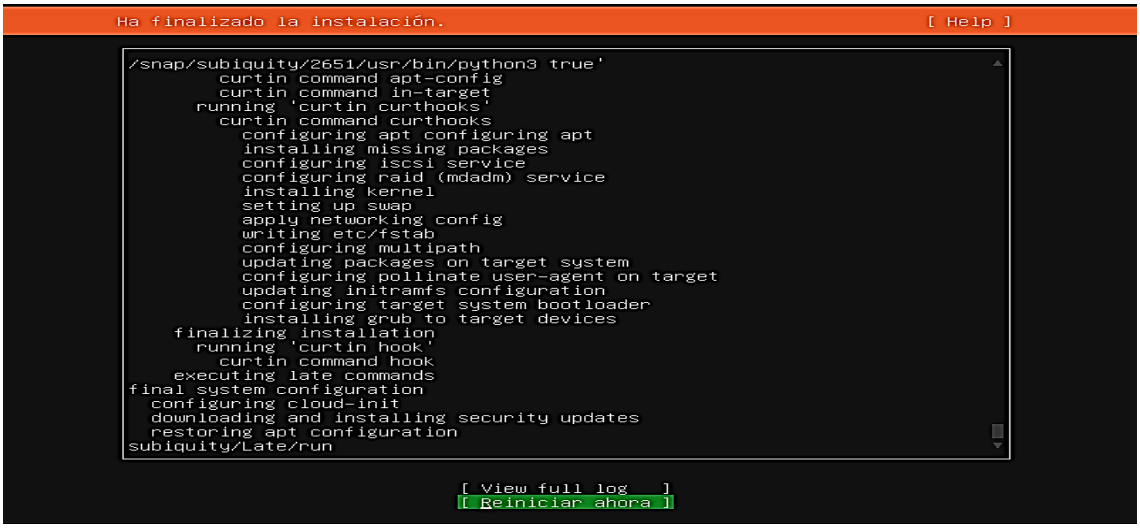
Configuración instantánea destacadas del servidor



Finalmente se muestra la ventana ha finalizado la instalación como se indica en la *figura 17*, luego se procede a dar clic en reiniciar ahora en donde se detienen algunos paquetes que no son necesarios.

Figura 17

Finalización de la instalación

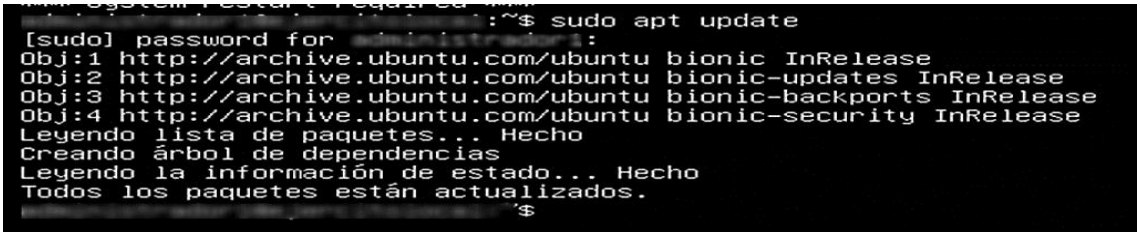


3.3.2. Actualización de paquetes

Consecuentemente para iniciar con la actualización de paquetes dentro de Ubuntu Server 18.04 LTS, se debe ejecutar el comando **sudo apt update** como se muestra en la *figura 18***,** el cual permite visualizar los repositorios que definimos en el archivo y se debe tener en cuenta que el comando no instala nada.

Figura 18

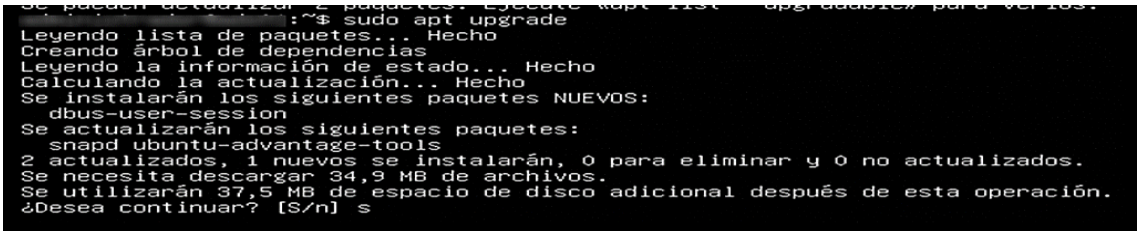
Comando sudo apt update



Luego se debe ejecutar el comando **sudo apt upgrade** como se muestra en la *figura 19*, el cual se encarga de actualizar todos los listados de paquetes disponibles en las fuentes definidas.

Figura 19

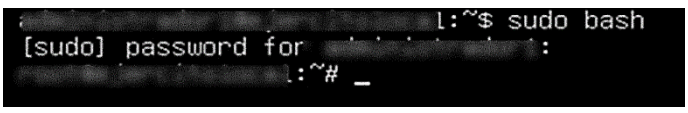
Comando sudo apt upgrade



Posteriormente, se ingresa el comando **sudo bash** como se indica en la *figura 20*, el cual permite realizar la ejecución de comando como super administrador.

Figura 20

Comando Sudo bash

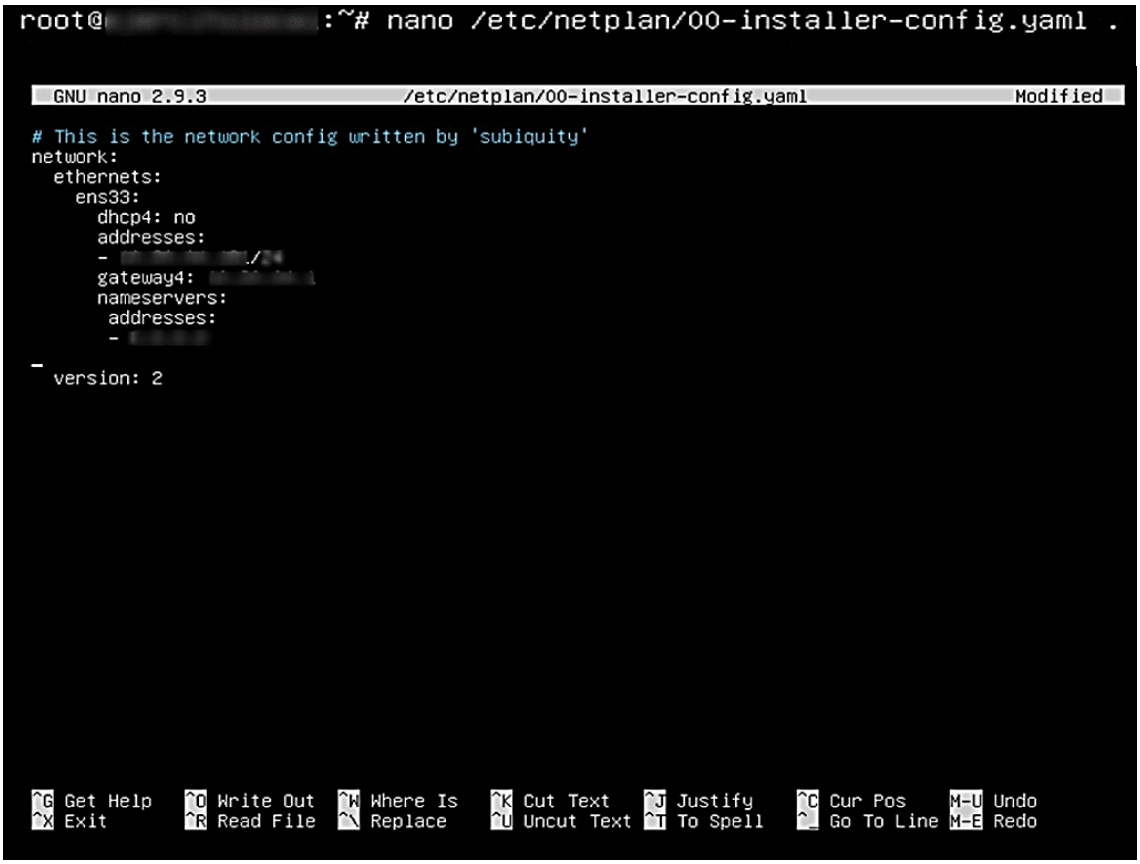


3.3.3. Configuración de la tarjeta de red

Inicialmente para la configuración de la tarjeta de red, se debe ejecutar el comando **nano /etc/netplan/00-installer-configurayaml** como se muestra en la *figura 21***,** el cual permite editar el archivo de plan de red predeterminado.

Figura 21

Configuración de tarjeta de red



Finalmente, para guardar la configuración de la tarjeta de red se utiliza la siguiente combinación de teclas: control + O, enter y control + X.

3.3.4. Verificación de la tarjeta de red

Se inicia al ejecutar el comando **netplan apply** como se indica en la *figura 22*, el cual permite aplicar la configuración de los archivos de la tarjeta de red.

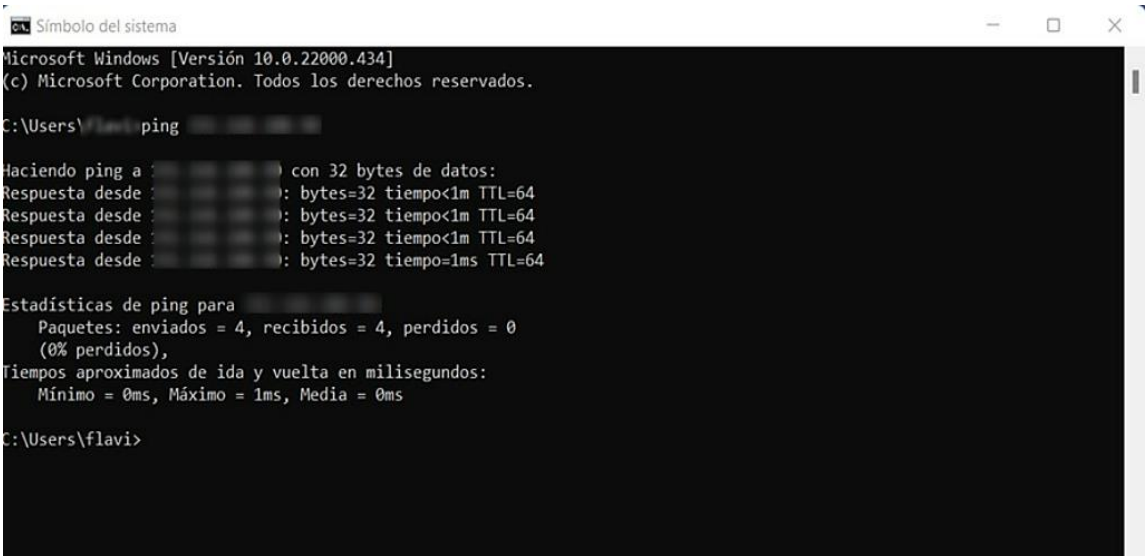
Figura 22

Comando netplan apply

Posteriormente, se ejecuta el comando **ping** como se muestra en la *figura 23***,** el cual permite comprobar si tiene conectividad con la configuración de la tarjeta de red.

Figura 23

Comando ping



3.3.5. Instalación del SSH

Se inicia al ejecutar el comando **netstat -tupan** como se indica en la *figura 24*, el cual permite revisar los puertos que están habilitados.

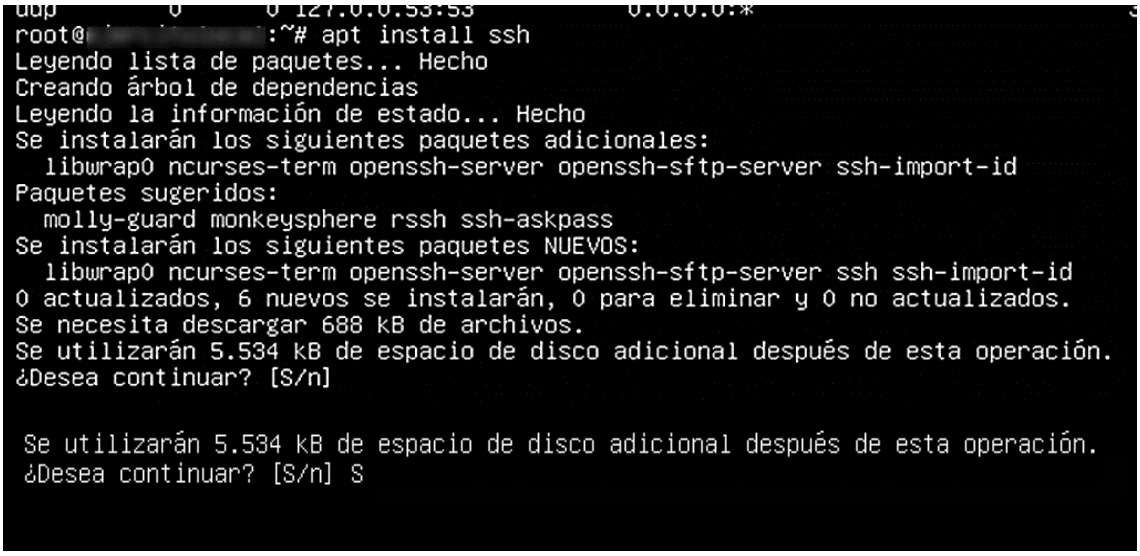
Figura 24

Comando netstat -tupan

Luego se debe ejecutar el comando **apt install ssh** como se muestra en la *figura 25***,** cuyo fin es instalar el repositorio para lograr el acceso remoto.

Figura 25

Comando apt install ssh



Posteriormente, se ejecuta nuevamente el comando **netstat -tupan** como se indica en la *figura 26*, el cual permite verificar los puertos que están habilitados con la instalación de acceso remoto.

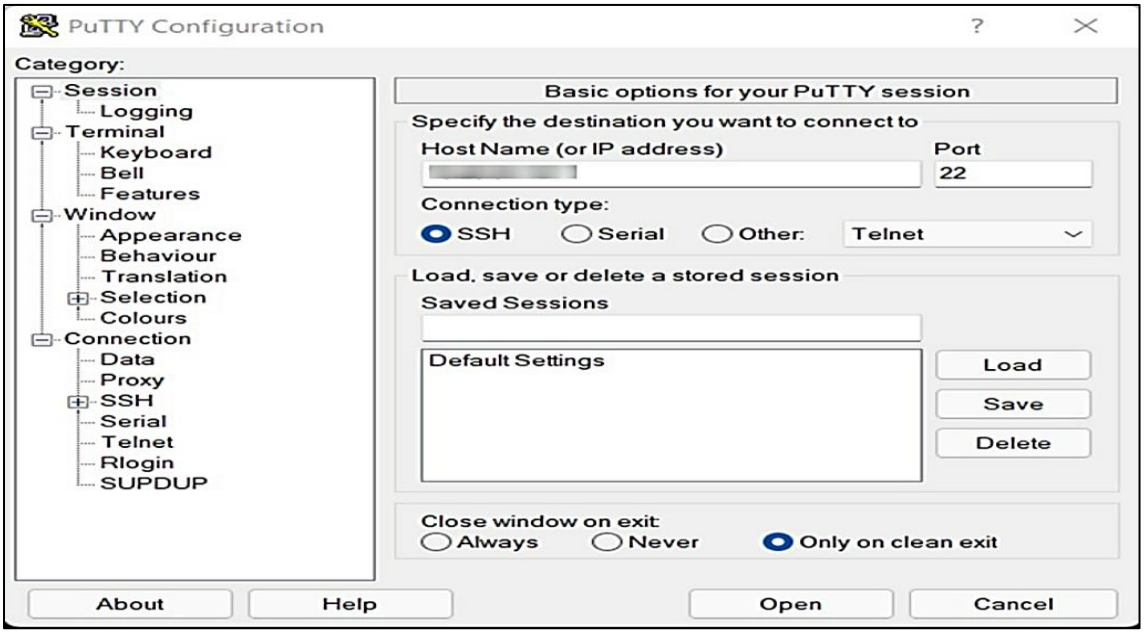
Figura 26

Comando netstat -tupan

Luego se debe ejecutar el software PuTTY como se muestra en la *figura 27*, con el fin de acceder de forma remota para obtener una configuración más rápida y eficiente. Teniendo en cuenta que este paso solo es una alternativa para una configuración más breve.

Figura 27

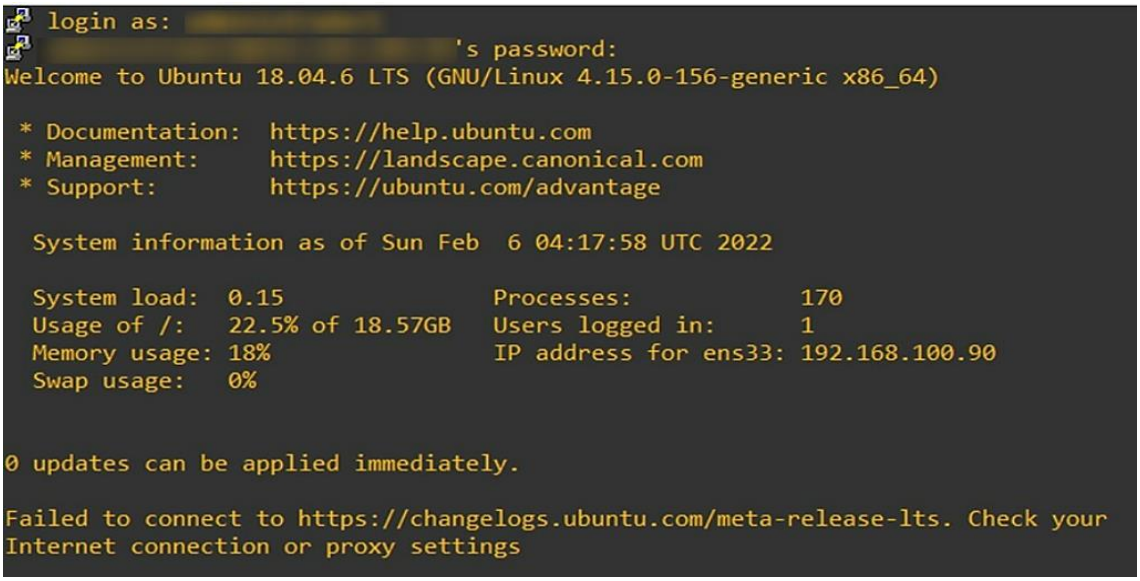
Acceso remoto



Luego de acceder de forma remota se debe ingresar el respectivo usuario y contraseña para tener acceso como administrador, como se indica en la *figura 28*, con el propósito de poder continuar con la instalación del controlador de dominio.

Figura 28

Acceso como administrador

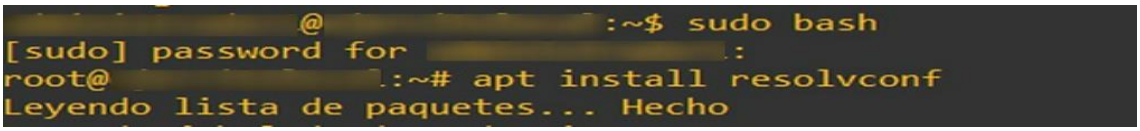


3.3.6. Configurar servidores de nombre DNS

Para iniciar con la configuración de servidores DNS, como se indica en la *figura 29*, se ingresa como super administrador con el comando sudo bash, luego se ejecuta el comando **apt install resolvconf** que permite configurar servidores de nombre DNS permanentes.

Figura 29

Biblioteca para DNS



Posteriormente se desactiva los DNS que se instala por defecto para el Active Directory como se indica en la *figura 30*, para lo cual se procede a la configuración de un DNS propio para el controlador de dominio, mediante la ejecución de los siguientes comandos:

- systemctl stop systemd-resolved
- systemctl disable systemd-resolved
- rm -rf /etc/resolv.conf

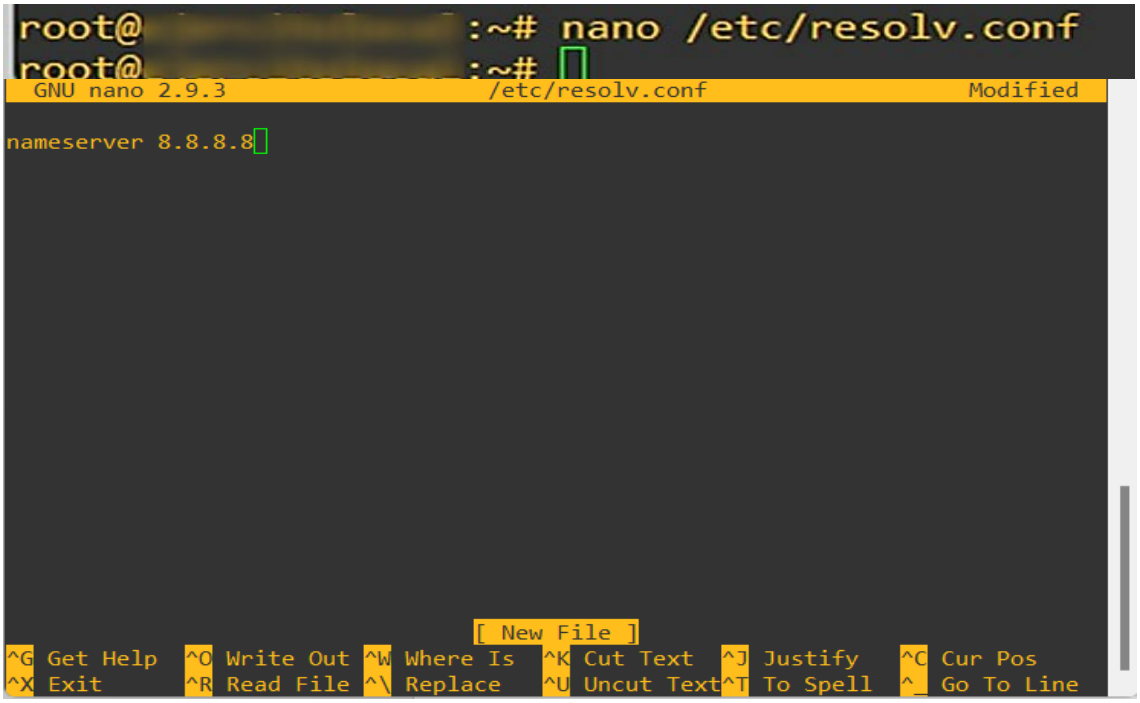
Figura 30

Desactivar DNS

Posteriormente se debe ejecutar el **comando nano /etc/resolv.conf** como se muestra en la *figura 31***,** donde se observa si el DNS se está resolviendo de una manera eficaz mediante la comprobación con el DNS del internet.

Figura 31

Agregar DNS de google



Posteriormente, para guardar la configuración del DNS de Google se presiona la siguiente combinación de teclas: control + O, enter y control + X.

Luego, se ejecuta el comando **ping** como se muestra en la *figura 32***,** el cual permite comprobar si tiene conectividad con el internet.

Figura 32

Comando ping

Luego, se ejecuta el comando **nano /etc/hosts** como se muestra en la *figura 33***,** el cual permite agregar el nombre del equipo como ads01 y el nombre del dominio que va a utilizar.

Figura 33

Comando nano /etc/hosts

Luego para guardar la configuración del nombre del equipo se presiona la siguiente combinación de teclas: control + O, enter y control + X.

Posteriormente se debe ejecutar el **comando nano /etc/hostname** como se muestra en la *figura 34***,** el cual se utiliza para realizar el cambio del nombre del dominio.

Figura 34

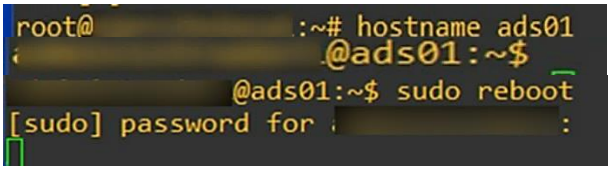
Comando nano /etc/hostname

Luego, para guardar el cambio de nombre se presiona la siguiente combinación de teclas: control + O, enter y control + X.

Finalmente, se ejecuta el comando **hostname ads01** como se muestra en la *figura 35,* el cual permite validar el nombre del dominio en ads01, posteriormente se ejecuta el comando **sudo reboot** que permite reiniciar el sistema con el fin de que se guarde la configuración.

Figura 35

Validación del nombre del dominio

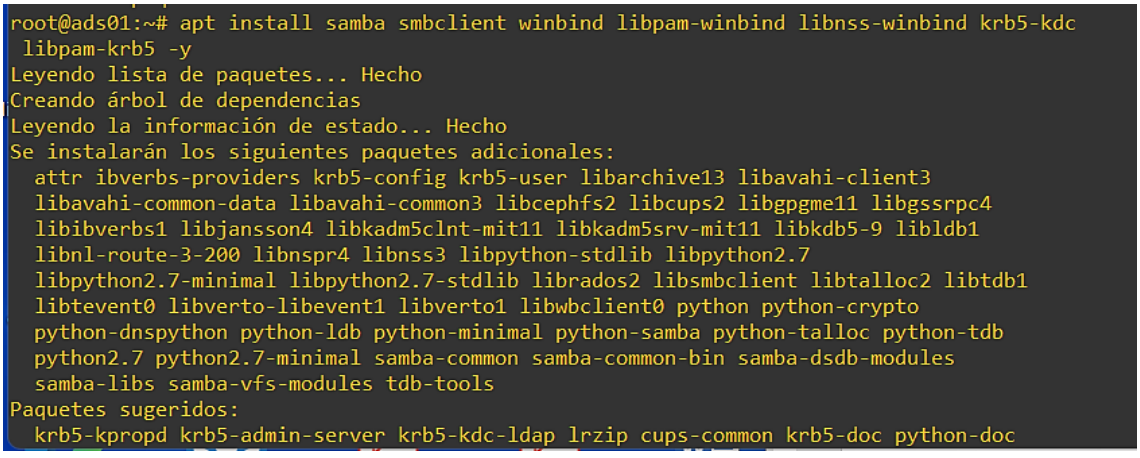


Instalación del servicio samba

Para iniciar con la instalación del servicio samba, como se indica en la *figura 36,* se debe ejecutar el comando **apt install samba smbclient winbind libpam-winbind libnss-winbind krb5-kdc libpam-krb5 -y**, aquel que permite realizar la instalación del paquete con los componentes necesarios, cuyo fin es tener la funcionalidad de un active directory. Además, se instala los servicios Ldap, de carpetas compartidas y DNS.

Figura 36

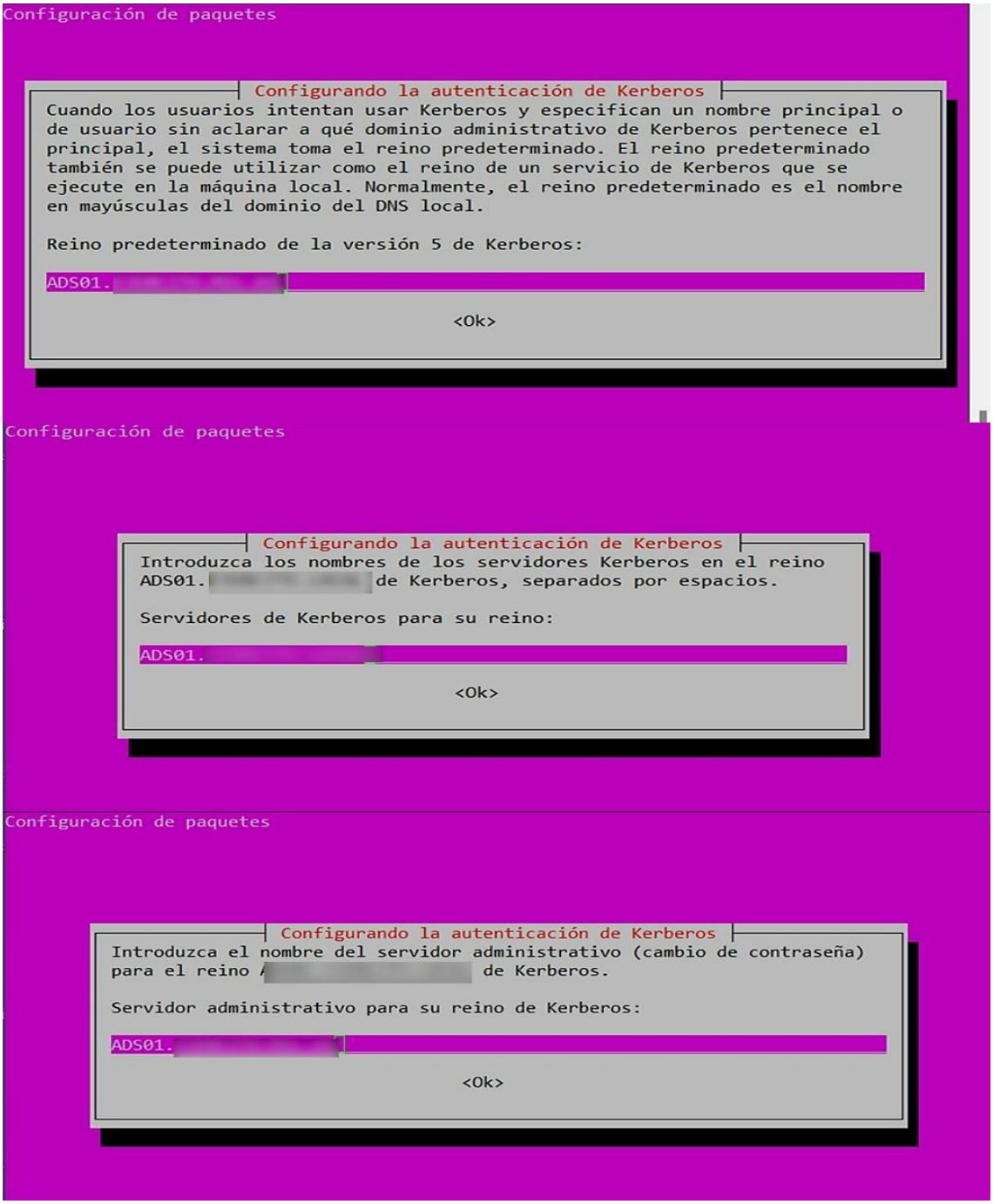
Instalación del servicio samba



Posteriormente, aparecen ventanas como se muestra en la *figura 37***,** en las cuales se debe realizar la configuración de los paquetes de autenticación de kerberos cuyo fin es lograr que tenga la funcionalidad de un active directory.

Figura 37

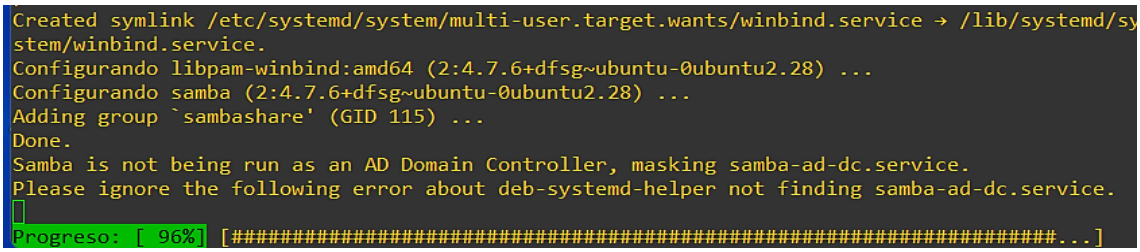
Configuración de los paquetes de kerberos



Luego, se muestra la ventana donde se visualiza el avance de la instalación del servicio samba como se muestra en la *figura 38,* con el fin de ayudar dentro de la funcionalidad de un controlador de dominio, tomando en cuenta que puede tardar varios minutos dependiendo de la velocidad del internet.

Figura 38

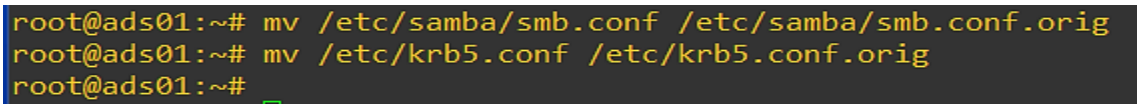
Avance de instalación samba



Luego, se ejecuta el comando **mv /etc/samba/smb.conf /etc/samba/smb.conf.orig** como se muestra en la *figura 39,* el cual permite mover los archivos cambiando su nombre ya que por lo general cuando están dentro de los archivos de configuración los “.com” son los archivos que guardan las configuraciones de lo backups. Posteriormente se ejecuta el comando **mv /etc/krb5.conf /etc/krb5.conf.orig,** que permite cambiar el nombre y poder identificar al archivo original.

Figura 39

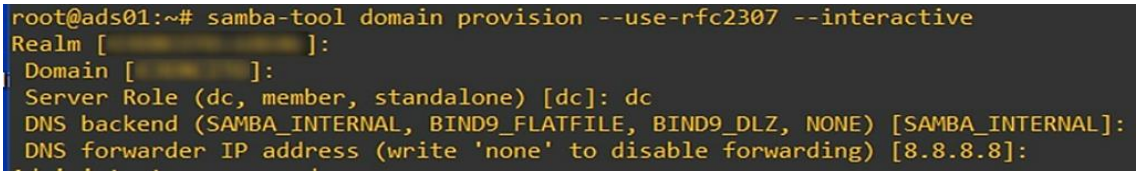
Mover carpetas de Krb5 backups



Posteriormente, se ejecuta el comando **samba-tool domain provision --use-rfc2307 --interactive** como se muestra en la *figura 40,* el cual permite realizar la instalación del servicio para el aprovisionamiento como active directory, teniendo en cuenta que aquí se procede a seleccionar el rol para el servidor, que para este caso es dc o más conocido como domain control o controlador de dominio.

Figura 40

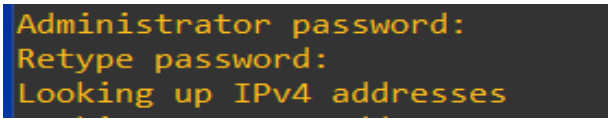
Rol del servidor



Luego, se debe asignar la clave de acceso para el administrador como se muestra en la *figura 41*, el mismo que tendrá el privilegio del control del contorno del controlador de dominio. Se debe tener muy en cuenta que la clave que se asigna para el administrator es única para el ingreso al controlador de dominio.

Figura 41

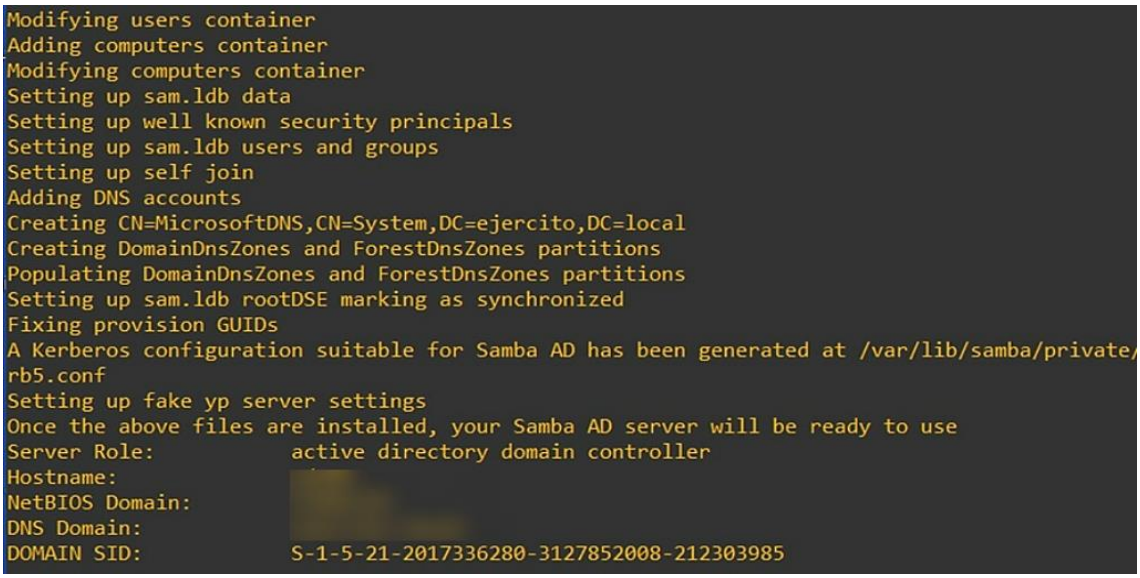
Asignar contraseña para el administrator



Posteriormente, se despliega una ventana como se indica en la *figura 42*, en la cual se observa cómo se crea el archivo kerberos con su respectiva estructura.

Figura 42

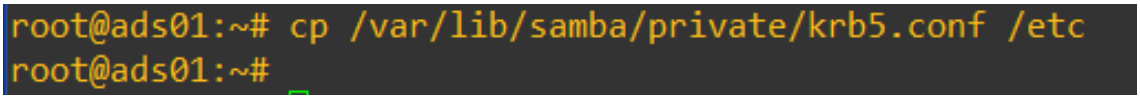
Estructura del archivo kerberos



Luego, se ejecuta el comando **cp /var/lib/samba/private/krb5.conf /etc** como se muestra en la *figura 43***,** el cual permite copiar el archivo kerberos krb5 a la carpeta del fichero etc.

Figura 43

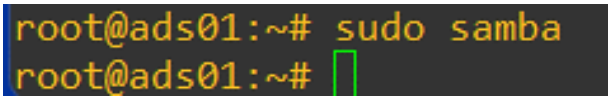
Copiar el archivo krb5 a la carpeta etc



Posteriormente, se ejecuta el comando **sudo samba** como se muestra en la *figura 44***,** el mismo que permite realizar un testeo para comprobar que se esté resolviendo bien la instalación de los ficheros.

Figura 44

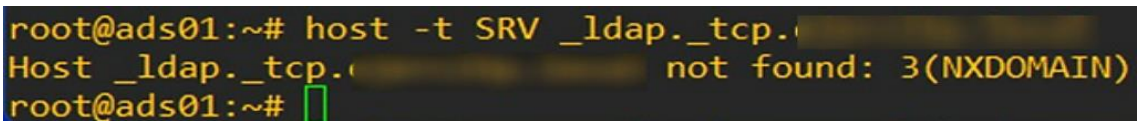
Testeo de ficheros



Luego, se ejecuta el comando **host -t SRV _ldap._tcp.“seguido del nombre del dominio”** como se muestra en la *figura 45***,** el cual permite realizar el testeo del servicio de DNS, el mismo que pregunta quién es el Ldap en donde se verifica como no encontrado ya que no se encuentra la dirección IP para el DNS.

Figura 45

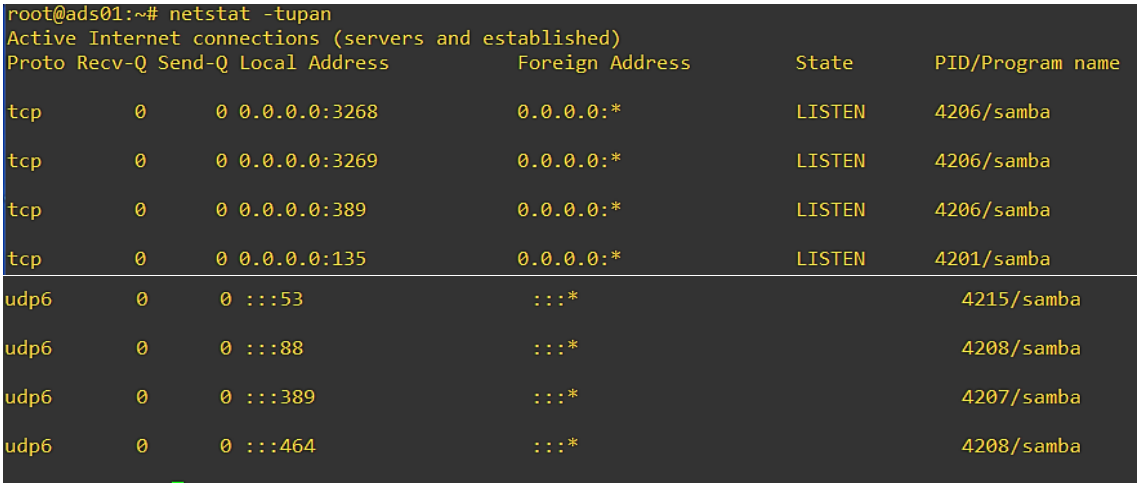
Comprobación del DNS del dominio



Posteriormente, se ejecuta el comando **netstat -tupan** como se muestra en la *figura 46***,** el cual permite revisar si se abrieron los servicios del active directory dando paso a los puertos que ayuda a la estructura, a la autenticación del Windows y compartición de las carpetas.

Figura 46

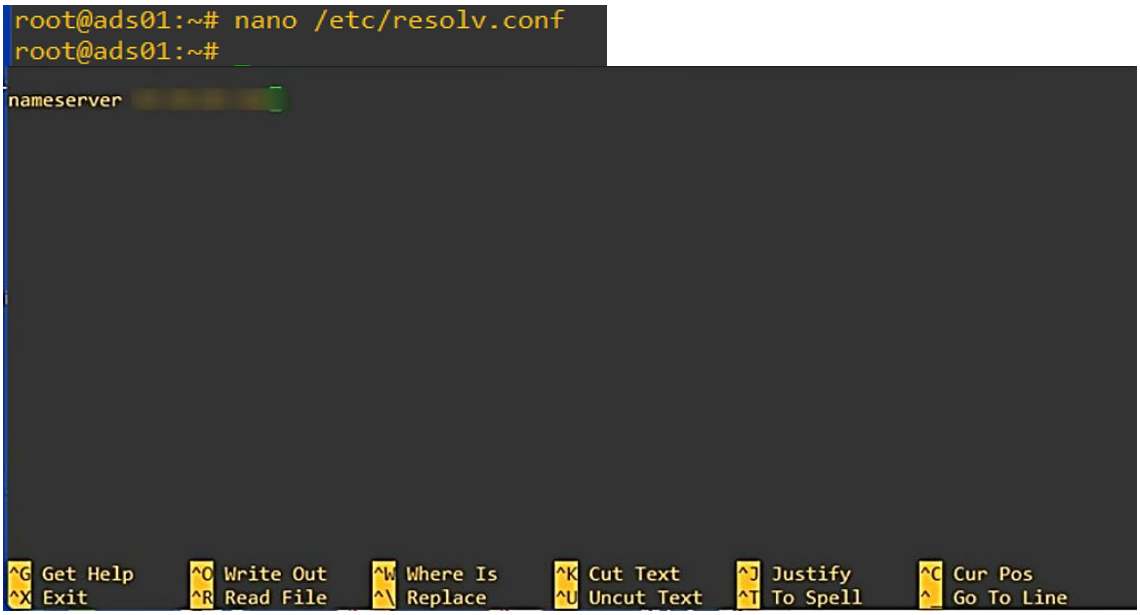
Verificación de los puertos



Luego, se ejecuta el comando **nano /etc/resolv.conf** como se muestra en la *figura 47***,** el cual permite cambiar el DNS para corregir el error de la consulta, el mismo que se encontraba seteado a Google.

Figura 47

Cambio de DNS



Posteriormente, para guardar la configuración del DNS del controlador de dominio se presiona la siguiente combinación de teclas: control + O, enter y control + X.

Finalmente, se ejecuta el comando **host -t SRV _ldap._tcp.ejercito.local** como se muestra en la *figura 48***,** el cual permite realizar el testeo del servicio de DNS, el mismo que pregunta quién es el Ldap en donde se puede visualizar que esta vez ya se encontró el DNS para el controlador de dominio.

Figura 48

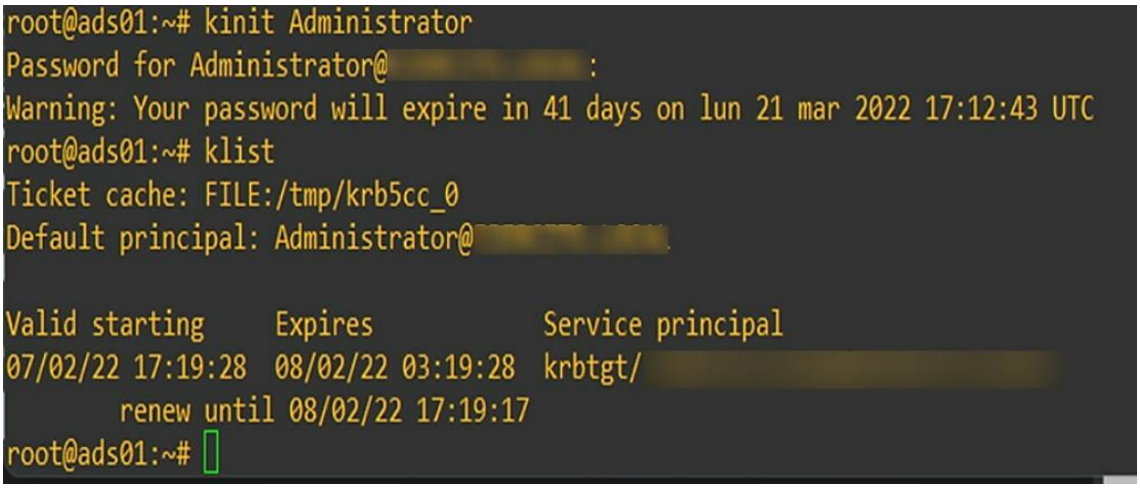
Verificación del Ldap

3.3.7. Comprobar el ticket del usuario

Para comprobar el ticket de usuario inicialmente se debe ejecutar el comando **kinit Administrator** como se muestra en la *figura 49***,** es aquel que realiza el testeo para verificar el usuario que se crea por defecto y ayuda a crear un ticket para cada usuario automáticamente; teniendo en cuenta que la primera vez se genera el usuario “administrator “de forma manual. Luego se ejecuta el comando **klist** el cual ayuda a enlistar los tickets existentes, teniendo en cuenta que para este caso solo se enlista el ticket principal “administrator”.

Figura 49

Comando kinit Administrator y klist



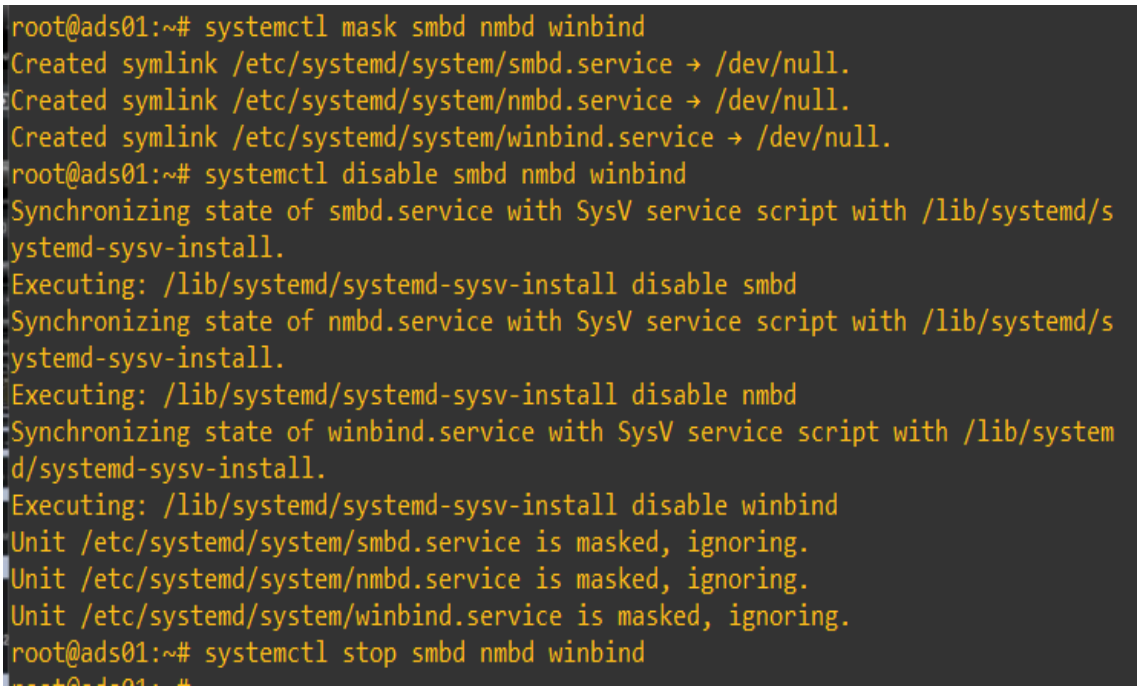
3.3.8. Activar los servicios del active directory

Para iniciar con la activación de los servicios del active directory se procede a desactivar los servicios innecesarios como se muestra en la *figura 50*, aquellos que son generados por defecto con la ayuda de los siguientes comandos:

- systemctl mask smbd nmbd winbind
- systemctl disable smbd nmbd winbind
- systemctl stop smbd nmbd winbind

Figura 50

Desactivar servicios innecesarios

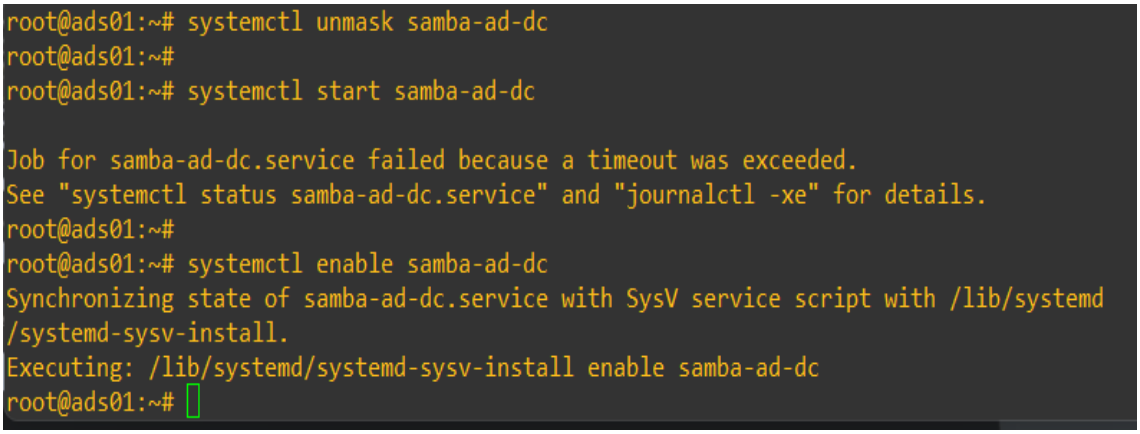


Luego, se procede activar el servicio automático como un active directory y los servicios de samba para un controlador de dominio como se muestra en la *figura 51***,** con la ayuda de los siguientes comandos:

- systemctl unmask samba-ad-dc
- systemctl start samba-ad-dc
- systemctl enable samba-ad-dc

Figura 51

Activación de servicios



Posteriormente, se ejecuta el comando **nano /etc/resolvconf/resolv.conf. d/tail** como se muestra en la *figura52***,** el cual permite cambiar el nombre del servidor con la dirección IP para el DNS del dominio.

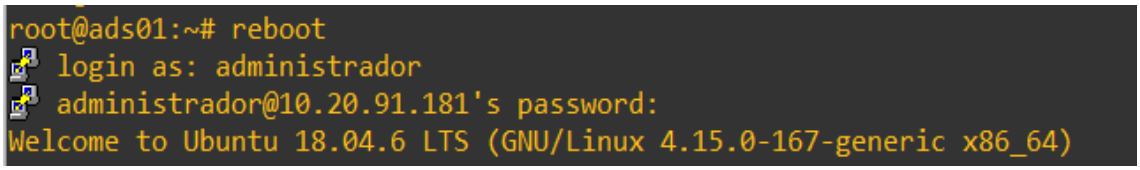
Figura 52

Cambio de nombre del dominio

Posteriormente, para guardar la configuración del nombre del controlador de dominio se presiona la siguiente combinación de teclas: control + O, enter y control + X. Luego, se ejecuta el comando **reboot** como se muestra en la *figura 53,* el cual permite reiniciar el servicio de samba como active directory.

Figura 53

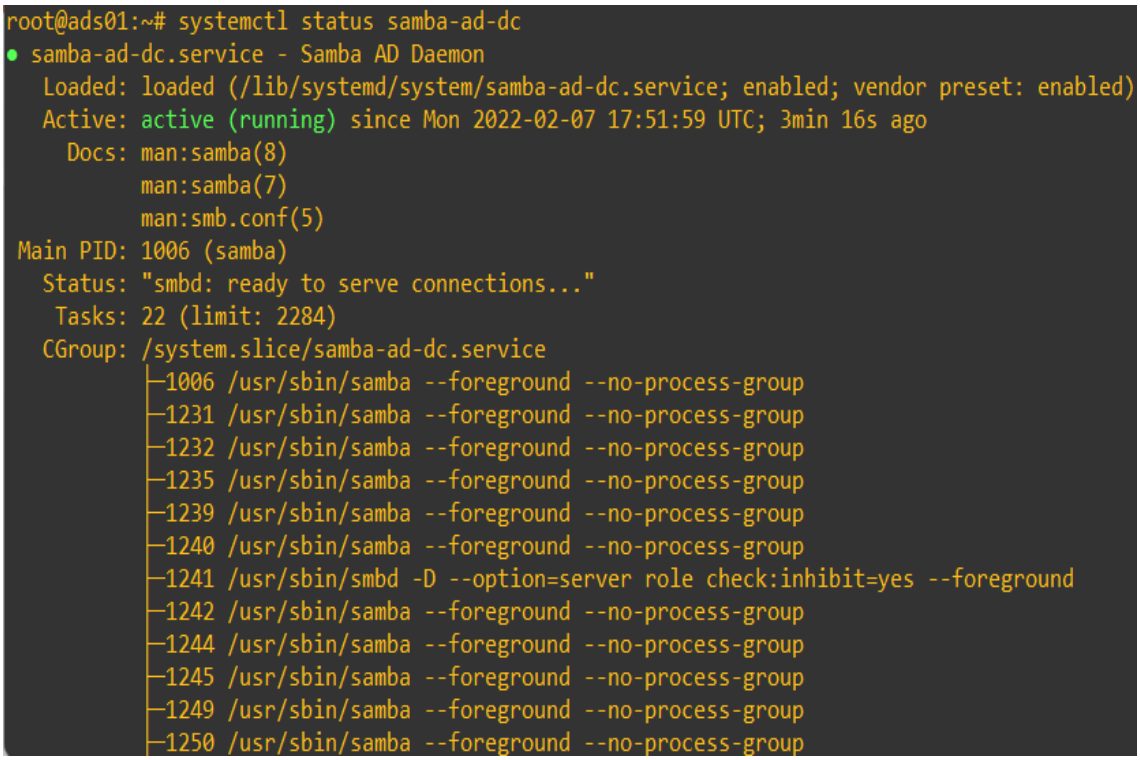
Comando reboot



Finalmente, se ejecuta el comando **systemctl status samba-ad-dc** como se muestra en la *figura 54,* el cual permite comprobar que se active de manera adecuada el controlador de dominio.

Figura 54

Activación del controlador de dominio

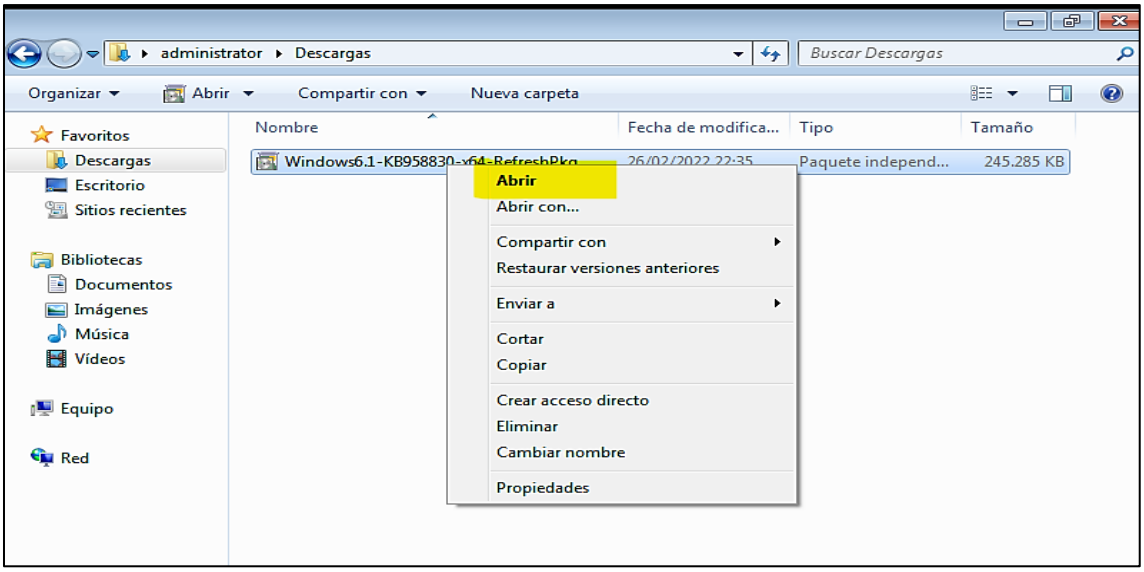


3.3.9. Instalación de la herramienta remota para Windows 6.1

Para iniciar con la instalación de la herramienta remota como se muestra en la *figura 55*, primero se debe descargar el software de la página oficial Windows 6.1-KB95830-x64, luego se debe dar clic derecho y seleccionar la opción abrir.

Figura 55

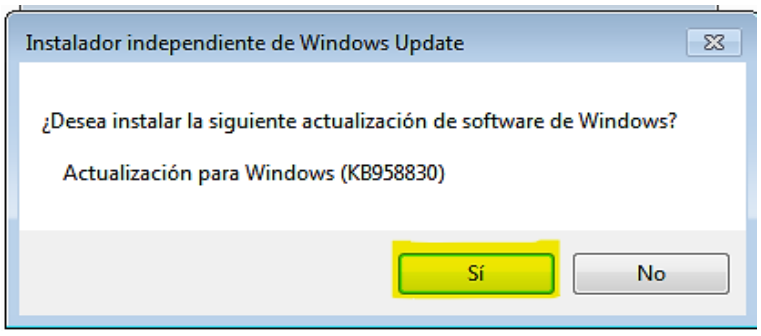
Abrir el software



Luego se despliega la ventana denominada instalador independiente de Windows update como se muestra en la *figura 56*, en la cual se debe dar clic en la opción sí para que se realice la actualización de Windows.

Figura 56

Actualización de Windows update



Posteriormente se despliega la ventana denominada descargar e instalar actualizaciones como se muestra en la *figura 57***,** en la cual se debe dar clic en acepto para aceptar cada una de las condiciones de instalación.

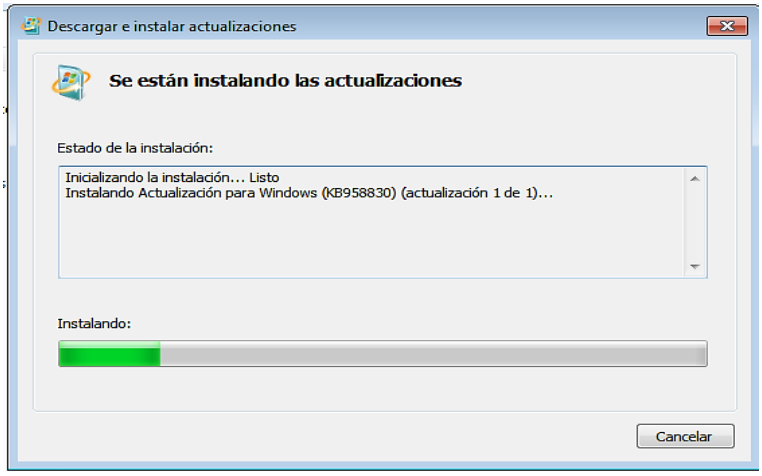
Figura 57

Condiciones de instalación

Luego se despliega la barra de avance de la instalación como se muestra en la *figura 58*, correspondiente a la herramienta de administración remota del servidor de Windows6.1-KB95830-x64.

Figura 58

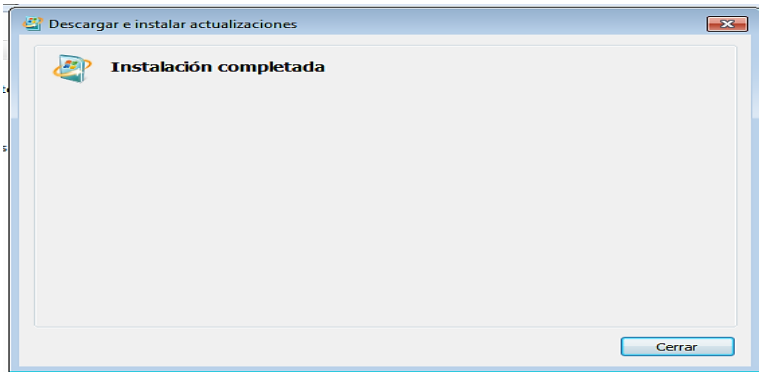
Barra de avance de instalación



Finalmente, se despliega la ventana instalación completa como se muestra en la *figura 59*, lo cual permite evidenciar que la herramienta de administración remota del servidor de Windows6.1-KB95830-x64 término de la manera adecuada.

Figura 59

Instalación completa

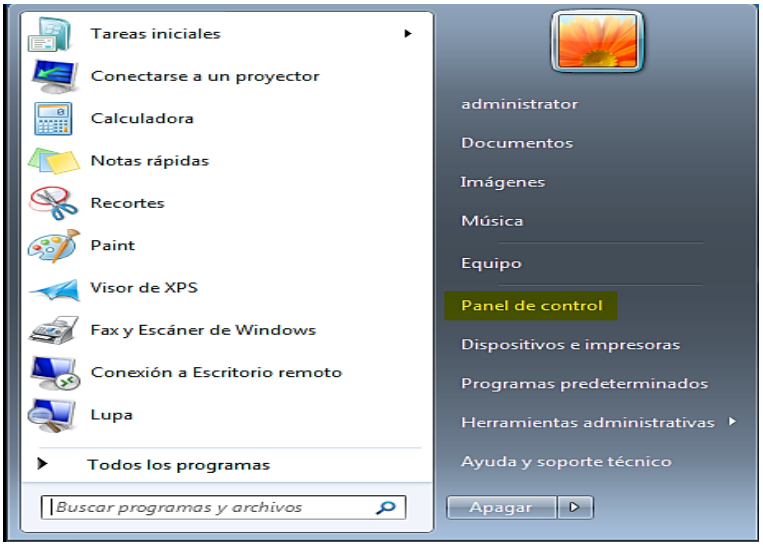


3.3.10. Activación de la herramienta remota para servidor de Windows 6.1

Para empezar con la activación de la herramienta remota para servidor de Windows 6.1-KB95830-x64 como se muestra en la *figura 60*, primero se dirige al panel de control.

Figura 60

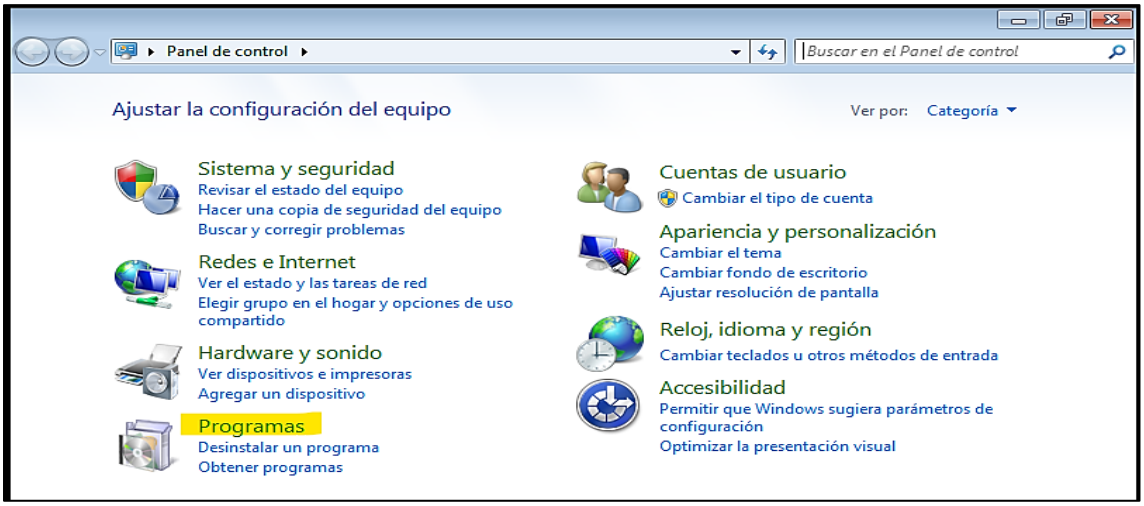
Panel de control



Luego se despliega la ventana panel de control como se muestra en la *figura 61*, en la cual se debe dar clic en la opción programas.

Figura 61

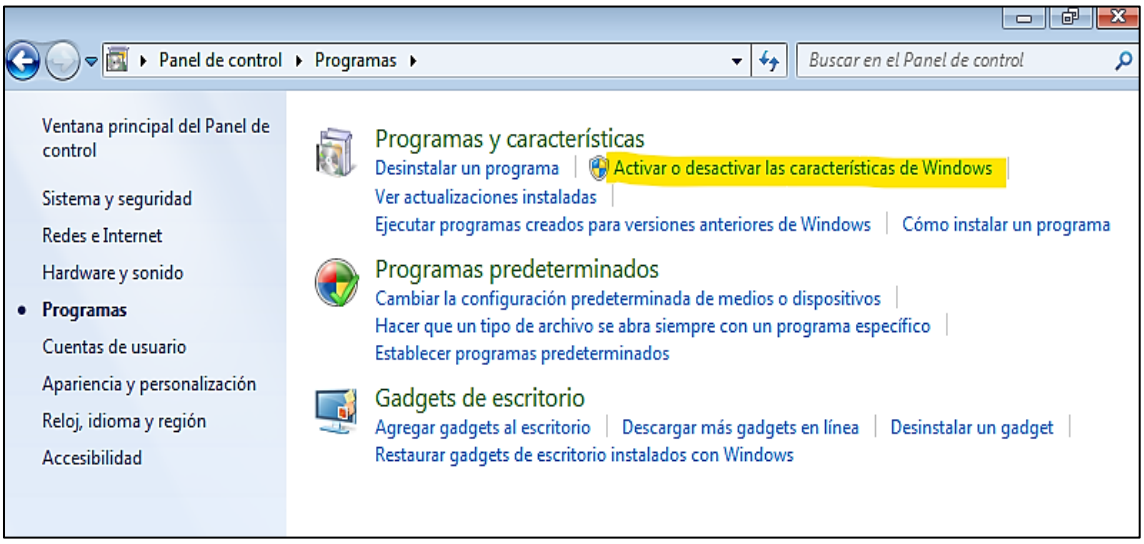
Icono programas



Posteriormente se despliega la ventana programas como se muestra en la *figura 62***,** en la cual se debe dar clic en la opción activar o desactivar las características de Windows.

Figura 62

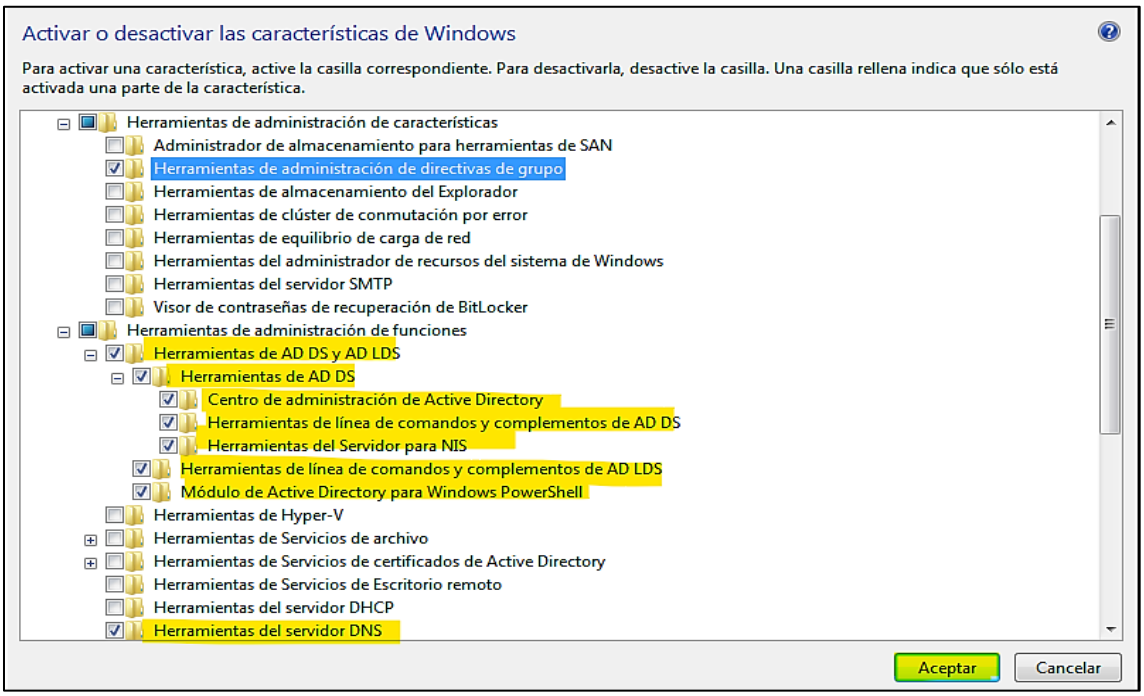
Activar o desactivar las características de Windows



Luego, se despliega la ventana característica de Windows como se muestra en la *figura 63*, en la que se debe tener en cuenta que la herramienta de administración remota del servidor requiere la activación de los siguientes parámetros y dar clic en aceptar.

Figura 63

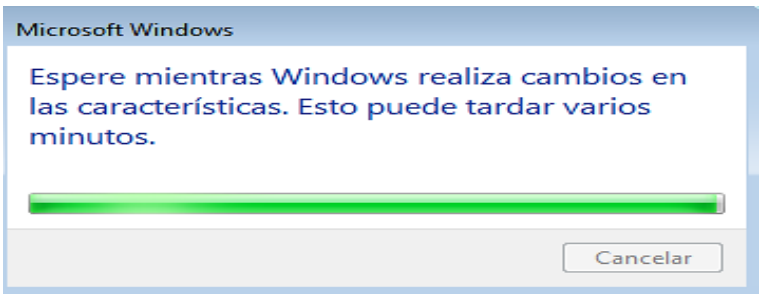
Activación de parámetros de Windows



Posteriormente se despliega la ventana Microsoft Windows como se muestra en la *figura 64***,** que muestra cómo se cargan los parámetros de la administración remota.

Figura 64

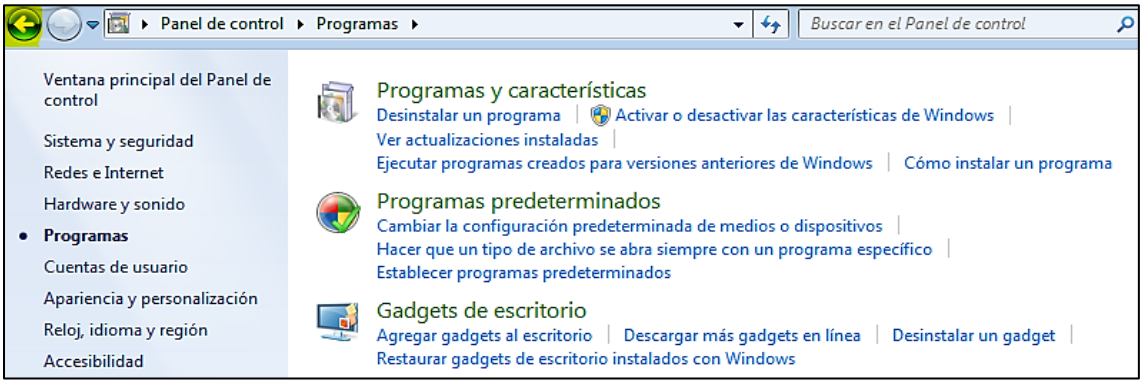
Parámetros de administración remota



Luego, se despliega nuevamente la ventana programas como se muestra en la *figura 65*, en la cual se debe dar clic atrás para poder regresar a la ventana panel de control.

Figura 65

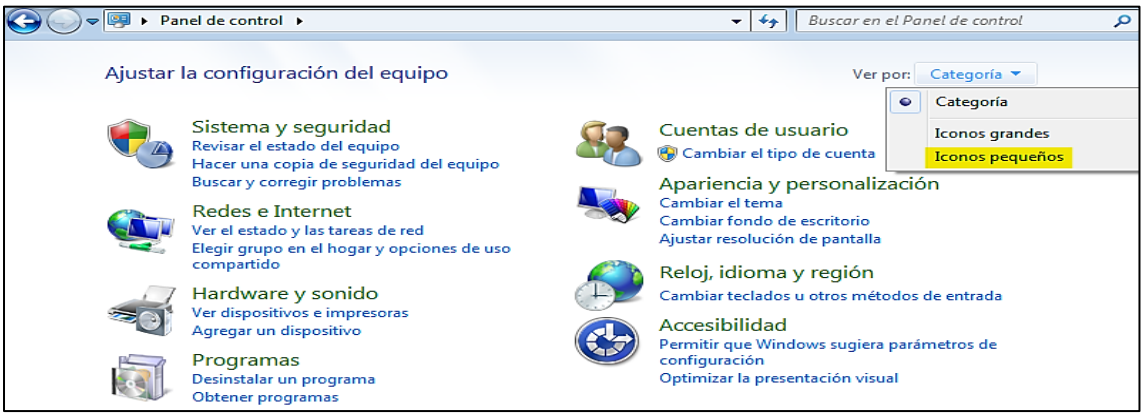
Icono programas



Posteriormente se despliega la ventana panel de control como se muestra en la *figura 66***,** en la cual se debe dar clic en la opción categoría y seleccionar iconos pequeños con el fin de mejorar la visualización.

Figura 66

Ajustar la configuración del equipo



Luego, se despliega la ventana ajustar la configuración del equipo como se muestra en la *figura 67***,** en la cual se debe dar clic en la opción herramientas administrativas.

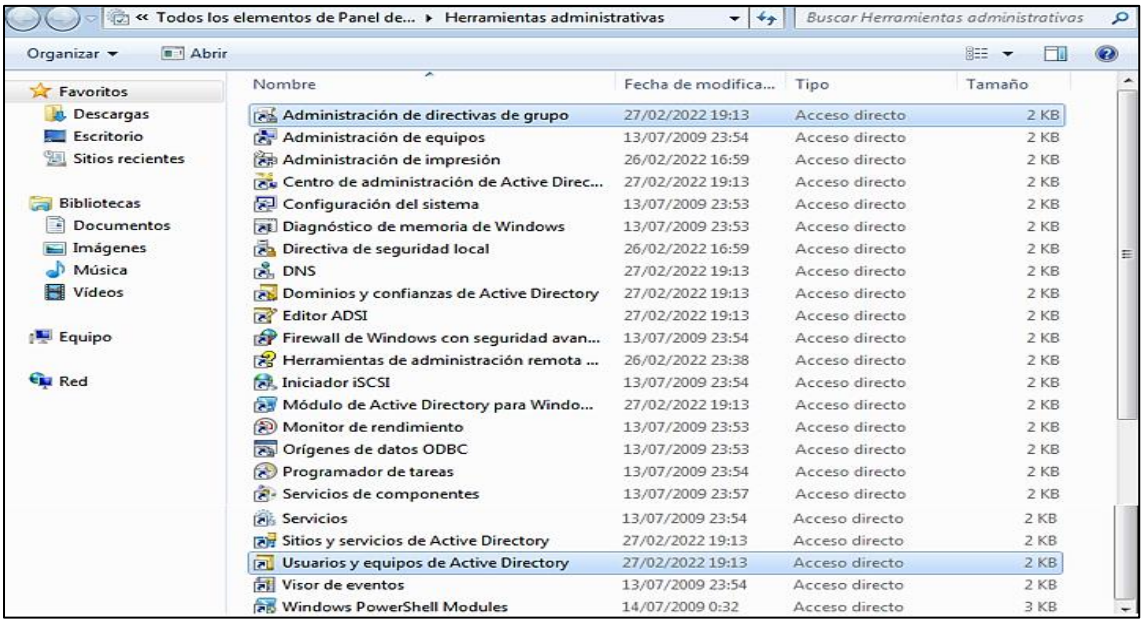
Figura 67

Ajustar la configuración del equipo

Posteriormente se despliega la ventana herramientas administrativas como se muestra en la *figura 68***,** en la cual se debe dar clic en la opción Administración de directivas de grupo que es la que permite crear las políticas de administración, luego dar clic en la opción usuarios y equipos del active directory que es aquella que permite crear la unidad organizativa y los usuarios.

Figura 68

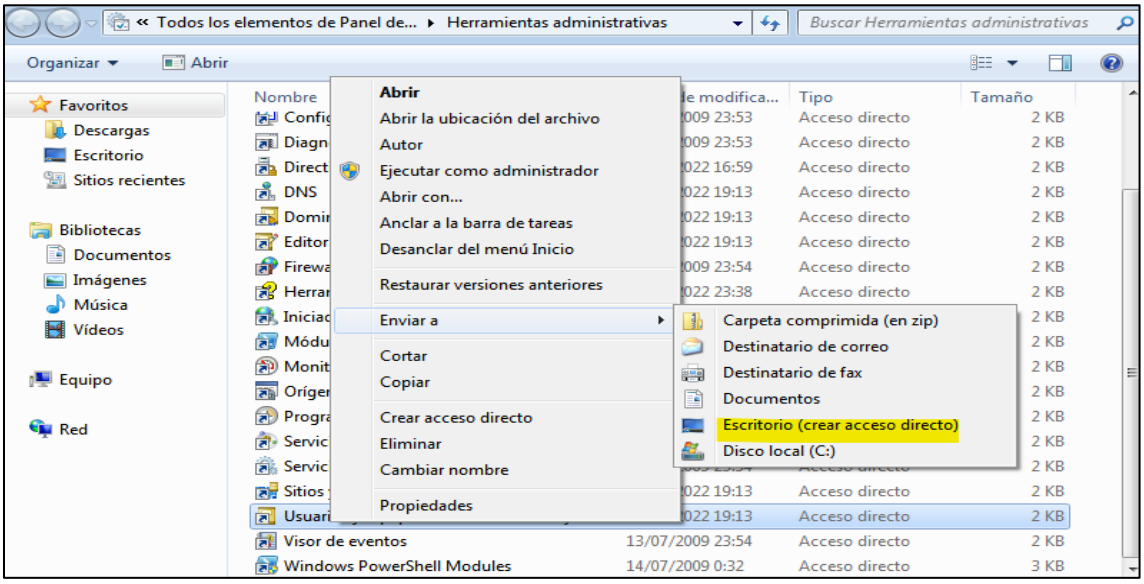
Herramientas administrativas



Luego, se despliega la ventana herramientas administrativas como se muestra en la *figura 69***,** en la cual se debe dar clic en la opción usuarios y equipos de un active directory y crear un acceso directo el cual permita acceder de manera más ágil y rápida.

Figura 69

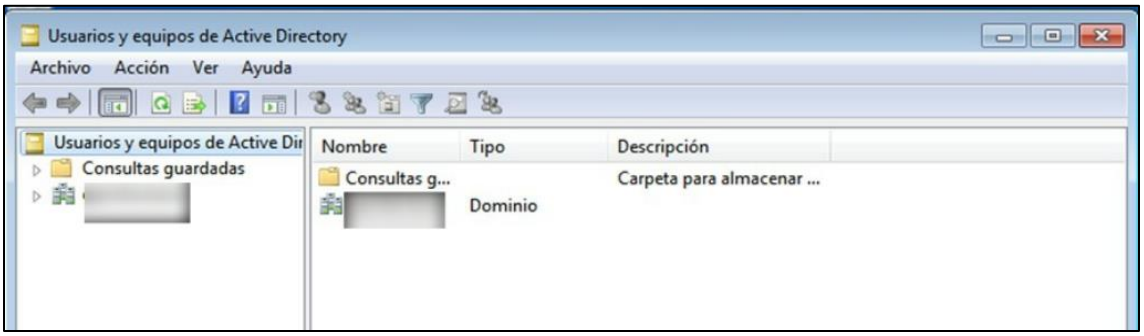
Acceso directo a usuarios y equipos



Posteriormente se despliega la ventana usuarios y equipos de active directory como se muestra en la *figura 70***,** aquí se puede visualizar la pantalla de administración remota de Windows para un directorio activo y también se procede a crear la unidad organizativa para el controlador de dominio.

Figura 70

Usuarios y equipos de active directory

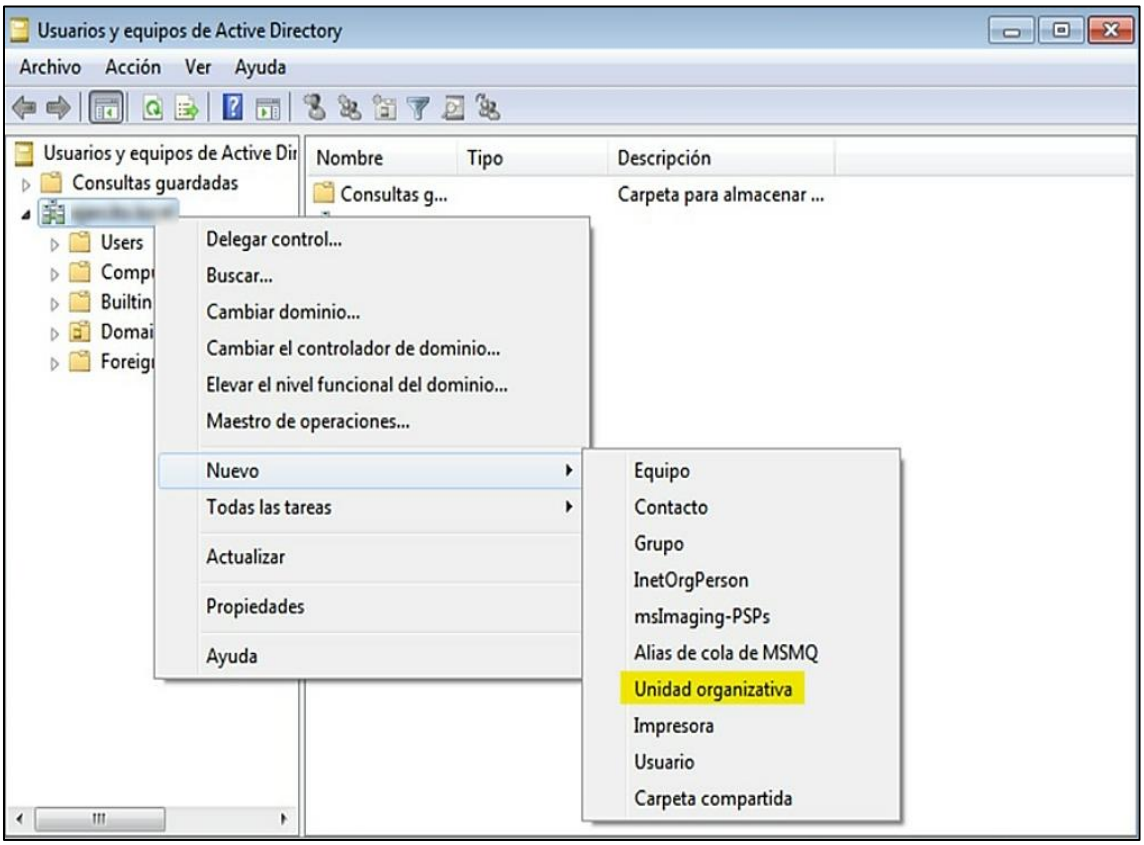


3.3.11. Crear la unidad organizativa (UO)

Para crear una unidad organizativa dentro del dominio de la CGFT como se muestra en la *figura 71***,** inicialmente se procede a dar clic derecho en el dominio, luego se selecciona la opción nueva y se escoge la unidad organizativa.

Figura 71

Creación de la unidad organizativa



Luego, se despliega la ventana nuevo objeto unidad organizativa como se muestra en la *figura 72***,** aquí se debe realizar el ingreso del nombre de la UO, que para este caso se crea la unidad de la CGFT y dar clic en aceptar. Tener muy en cuenta que debe estar activada la opción proteger contenedor contra eliminación accidental.

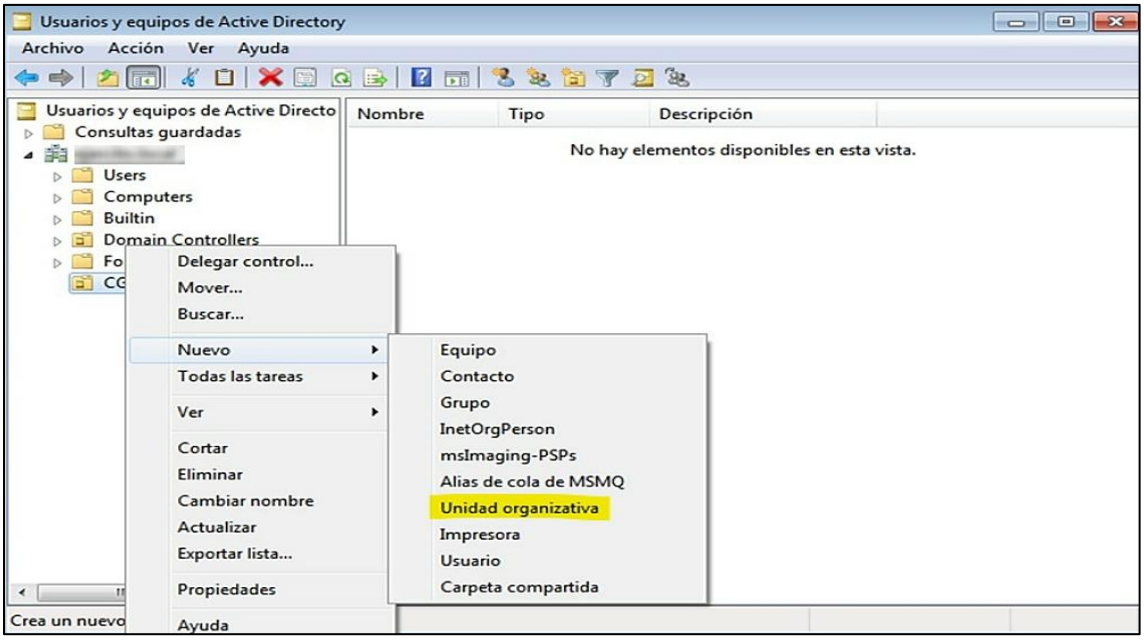
Figura 72

Ingreso del nombre de la UO

Posteriormente se despliega la ventana usuarios y equipos de active directory como se muestra en la *figura 73***,** aquí se crear una subunidad organizativa dentro de otra UO, la cual permite gestionar cada uno de los departamentos de la CGFT, para ello se procede a dar clic derecho en el dominio, seleccionar la opción nuevo y escoger unidad organizativa.

Figura 73

Creación de una subunidad organizativa



Finalmente, se despliega la ventana nuevo objeto unidad organizativa como se muestra en la *figura 74***,** aquí se debe realizar el ingreso del nombre de la subunidad UO que para este caso se crea el Departamento de las TIC´s de la CGFT y clic en aceptar.

Figura 74

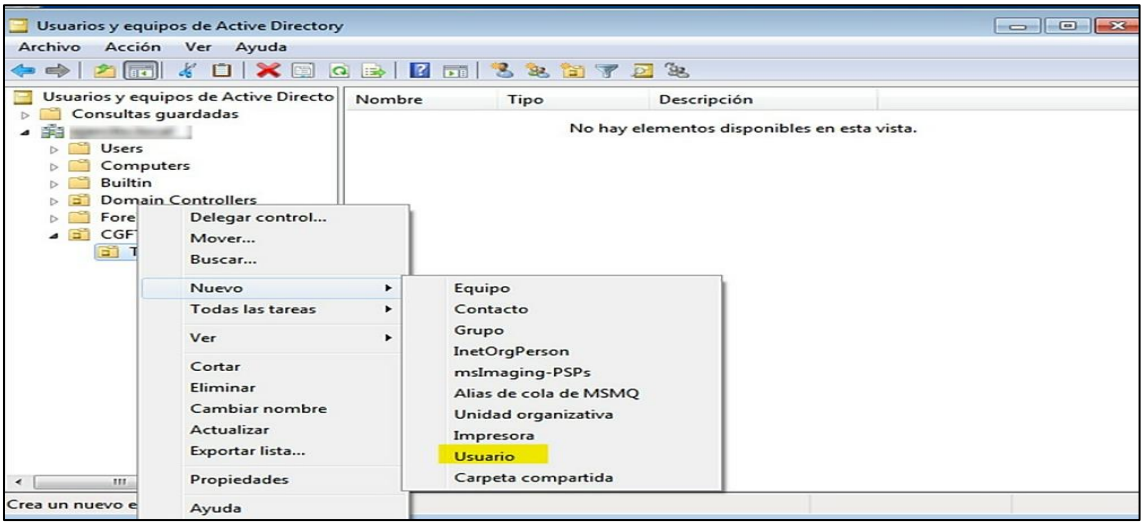
Nombre de la subunidad organizativa

3.3.12. Crear un usuario

Inicialmente para crear un usuario dentro de la UO se debe encontrar en la ventana usuarios y equipos de active directory como se muestra en la *figura 75***,** seleccionar la unidad organizativa que se creó en este caso es TIC´s, clic derecho, seleccionar nuevo y escoger la opción usuario.

Figura 75

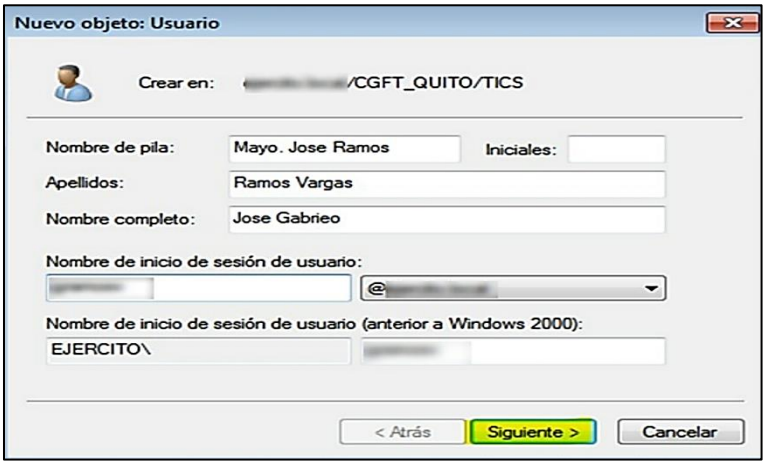
Creación del usuario



Posteriormente se despliega la ventana nuevo objeto usuario como se muestra en la *figura 76***,** en donde se deben ingresar los datos del nuevo usuario llenando cada uno de los campos luego dar clic en el botón siguiente.

Figura 76

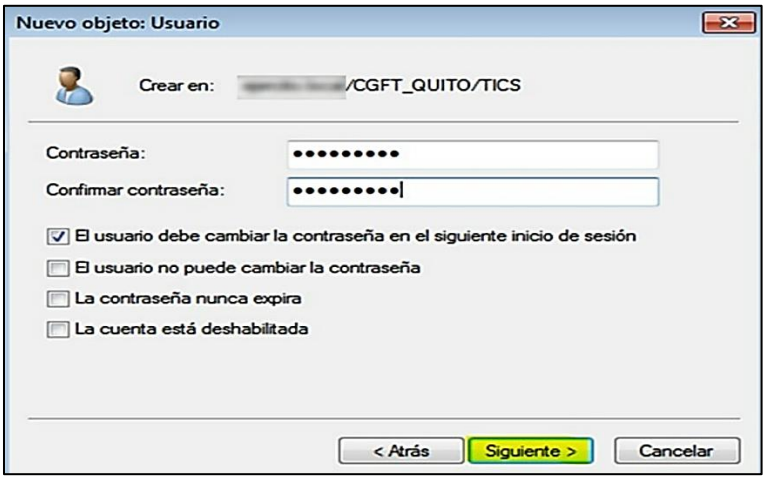
Ingreso de datos para el nuevo usuario



Luego, en la misma ventana nuevo objeto usuario como se muestra en la *figura 77***,** es necesario que se le asigne una contraseña la misma que tiene que cumplir con ciertos parámetros predeterminados, teniendo en cuenta que se debe activar la primera opción para que el usuario pueda cambiar la contraseña al inicio de sesión.

Figura 77

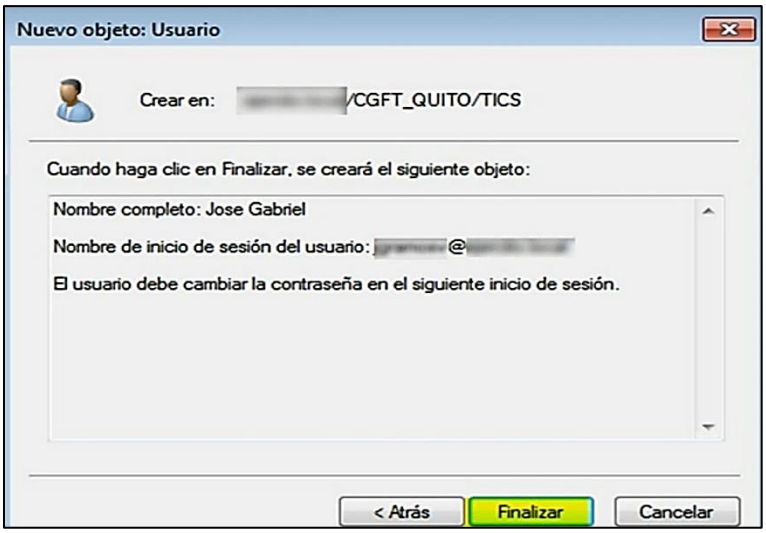
Asignación de la contraseña



Posteriormente se despliega la ventana con la información del usuario creado como se muestra en la *figura 78***,** y para terminar se debe dar clic en el botón finalizar.

Figura 78

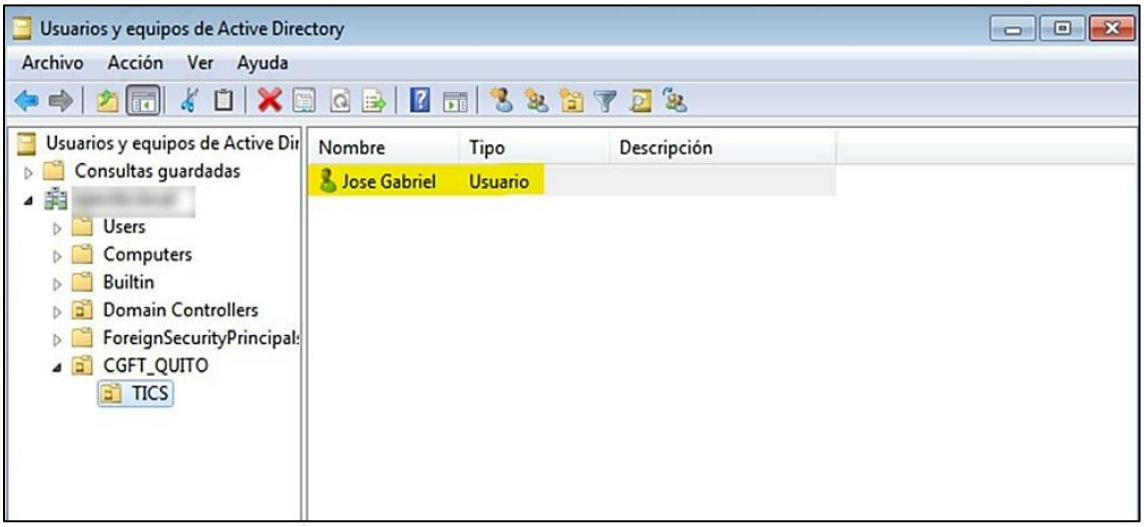
Información del usuario creado



Finalmente, se despliega la ventana usuarios y equipos de un active directory como se muestra en la *figura 79***,** en la cual se puede evidenciar la creación de usuario dentro de la UO de TIC´s.

Figura 79

Usuario creado dentro de la UO de TIC´s



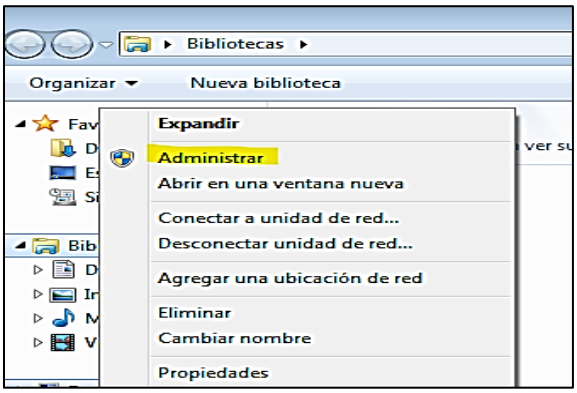
3.3.13. Ingresar un equipo al dominio

Habilitar la cuenta de administrador local

Para iniciar con la habilitación de la cuenta de administrador local del equipo como se indica en la *figura 79***,** primero se dirige a equipo ahí se da clic derecho y posteriormente clic en administrar.

Figura 80

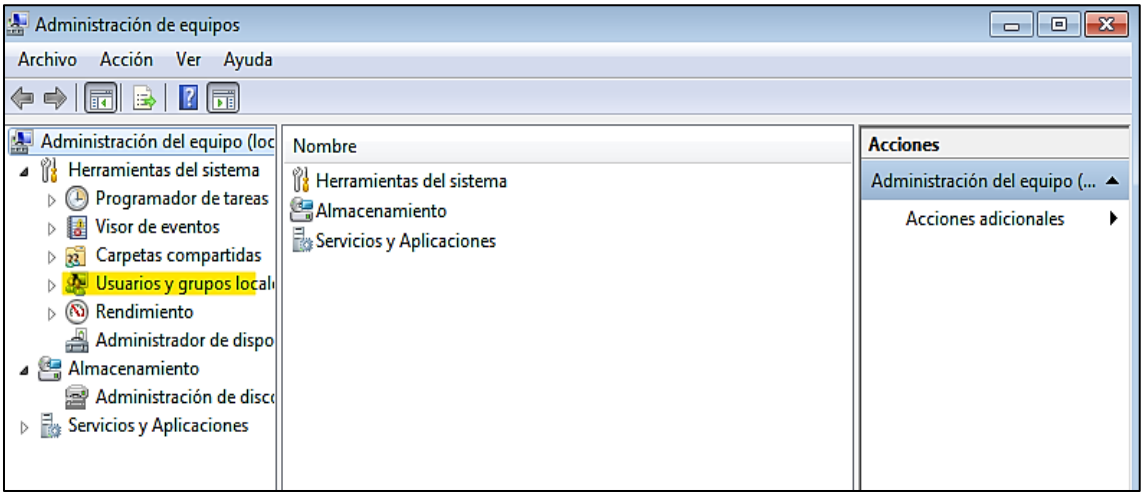
Habilitar cuenta de administración local



Posteriormente se despliega la ventana administración de equipos como se muestra en la *figura 81***,** en la cual se debe seleccionar la opción herramientas de sistemas y luego dar clic en usuarios y grupos locales.

Figura 81

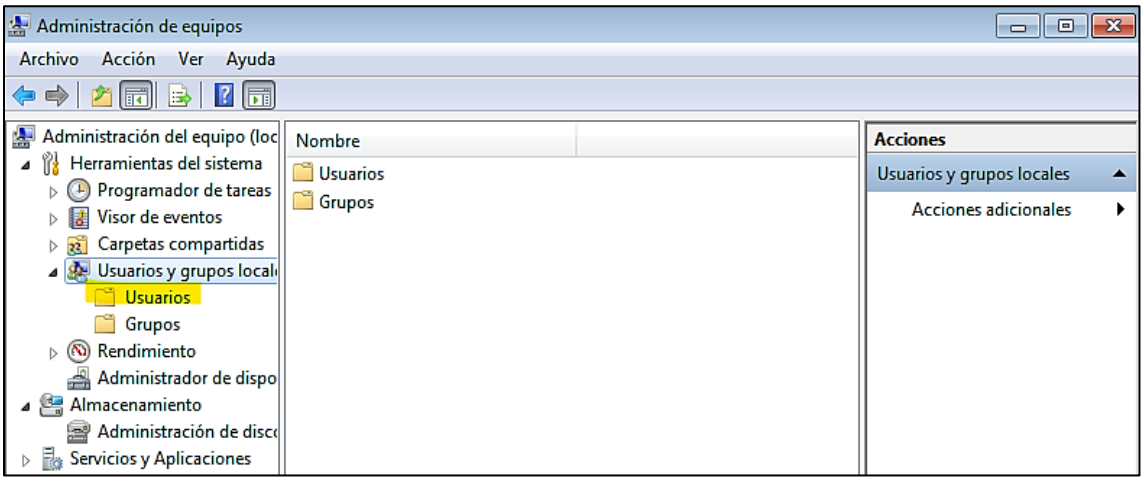
Administración de equipos



Luego, en la misma ventana administración de equipos como se muestra en la *figura 82***,** seleccionar la opción usuarios y grupos locales después dar clic en la opción usuarios.

Figura 82

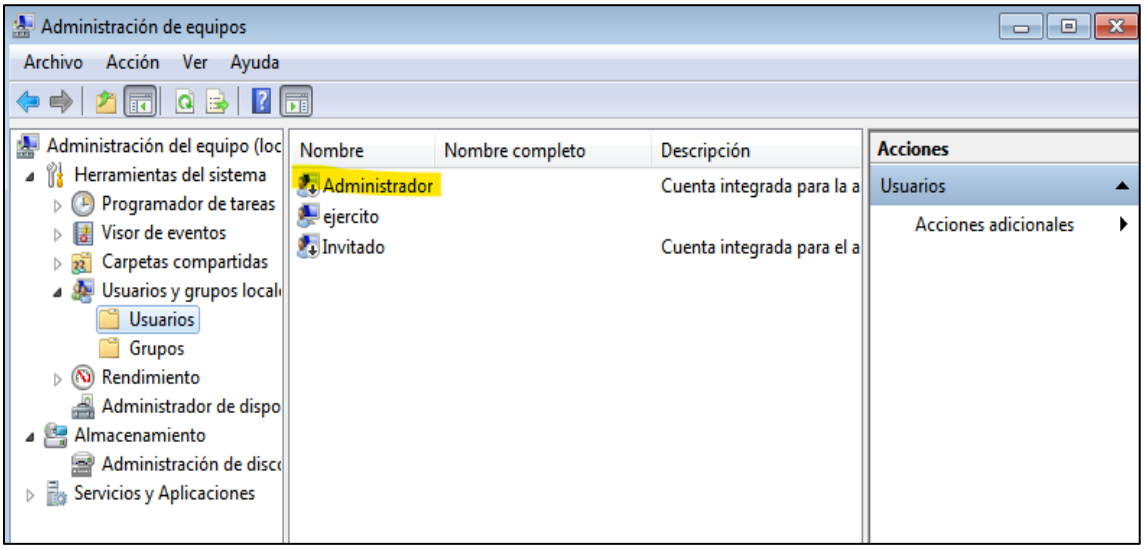
Carpeta usuarios



Posteriormente, en la misma ventana administración de equipos como se muestra en la *figura 83***,** teniendo en cuenta que en la parte derecha de la pantalla se puede visualizar la lista de usuarios locales y dar clic sobre la cuenta administrador.

Figura 83

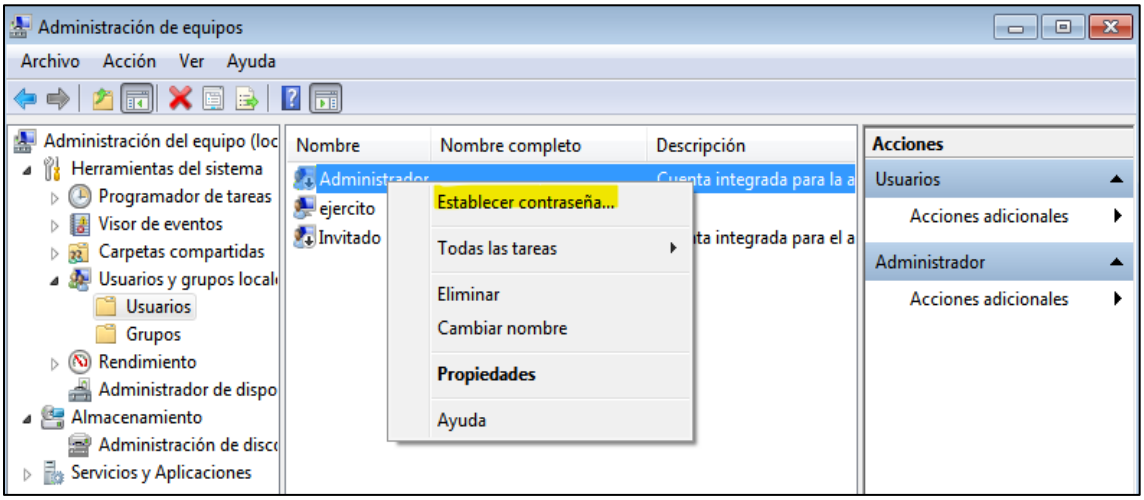
Cuenta del administrador



Luego, en la misma ventana administración de equipos como se muestra en la *figura 84***,** dar clic derecho en administrador y se despliega una ventana en la cual se elige la opción establecer contraseña.

Figura 84

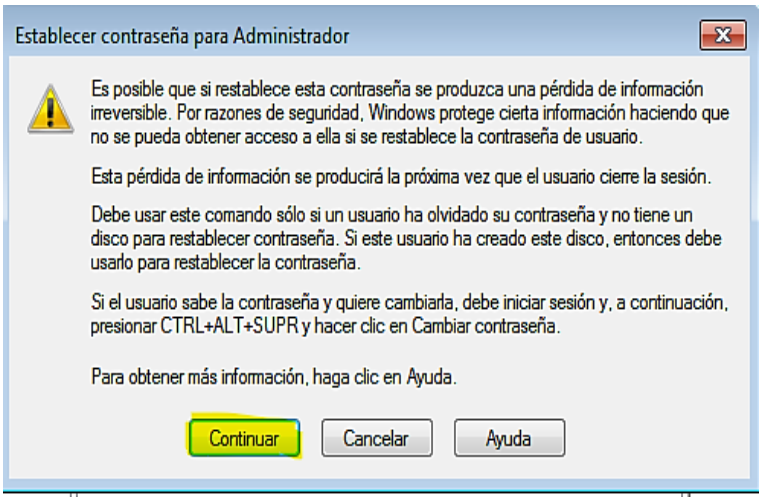
Establecer contraseña



Posteriormente, en la misma ventana establecer contraseña como se muestra en la *figura 85***,** se despliega una pantalla de advertencia notificando que puede existir una pérdida de información para esto procedemos a dar clic en continuar.

Figura 85

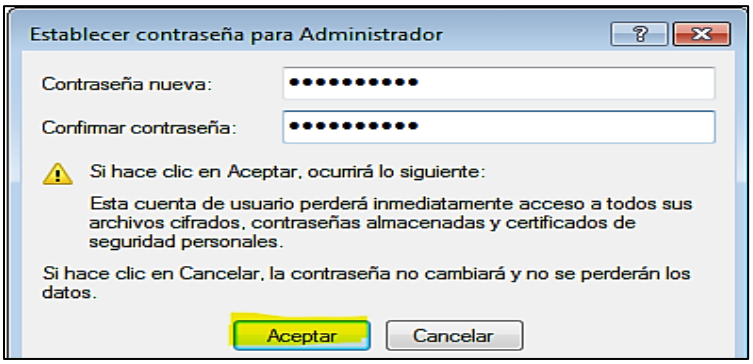
Establecer contraseña para administrador



Luego, en la misma ventana administración de equipos como se muestra en la *figura 86*, se despliega una ventana que permitirá ingresar la clave del administrador local, teniendo en cuenta que en este paso se sugiere estandarizar la clave en todos los equipos, la misma que no debe ser compartida por ningún motivo con los usuarios de la institución únicamente debe ser usada por el personal autorizado.

Figura 86

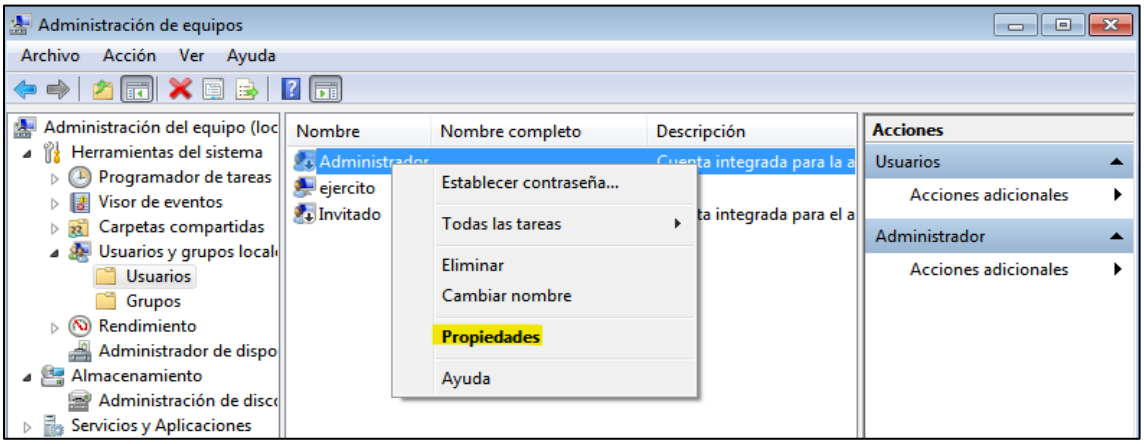
Clave del administrador local



Posteriormente, luego de cambiar la clave en administrador local como se muestra en la *figura 87***,** se debe habilitar la cuenta ya que por defecto se encuentra deshabilitada. Para lo cual se procede habilitar la cuenta dando clic derecho en administrador y se selecciona la opción propiedades.

Figura 87

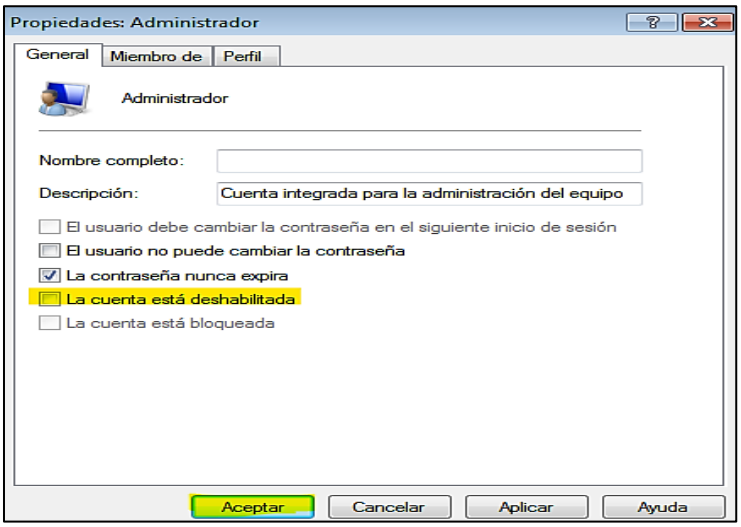
Propiedades de la cuenta



Finalmente, se despliega la ventana propiedades administrador como se muestra en la *figura 88***,** aquí se procede a desmarcar la opción la cuenta esta deshabilitada y dar clic en aceptar.

Figura 88

Habilitar cuenta

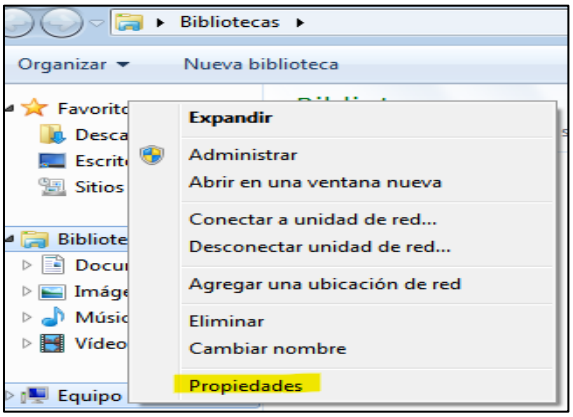


Cambiar el nombre del equipo

Para iniciar con el cambio de nombre del equipo se debe dar clic en equipo como se muestra en la *figura 89***,** en la cual se despliega una ventana que se escoge la opción propiedades.

Figura 89

Cambio de nombre del equipo



Posteriormente, en la ventana de información básica del equipo como se muestra en la *figura 90***,** en la inferior derecha se procede a seleccionar la opción cambiar configuración.

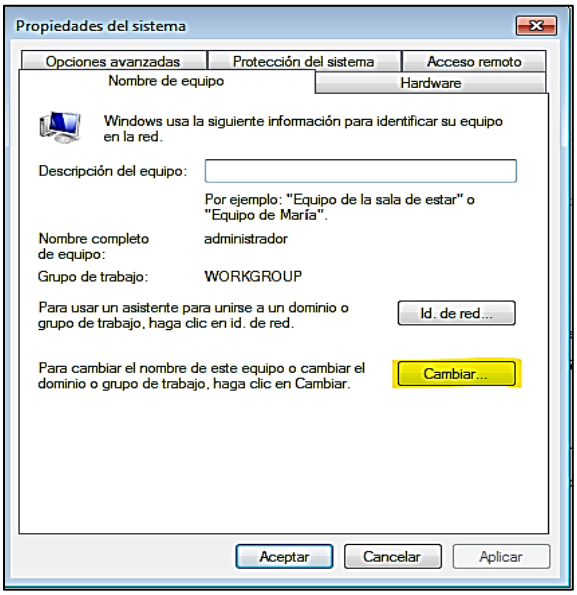
Figura 90

Cambiar configuración del equipo

Luego, se despliega la ventana propiedades del sistema como se muestra en la *figura 91*, en la cual se debe dar clic en la opción cambiar.

Figura 91

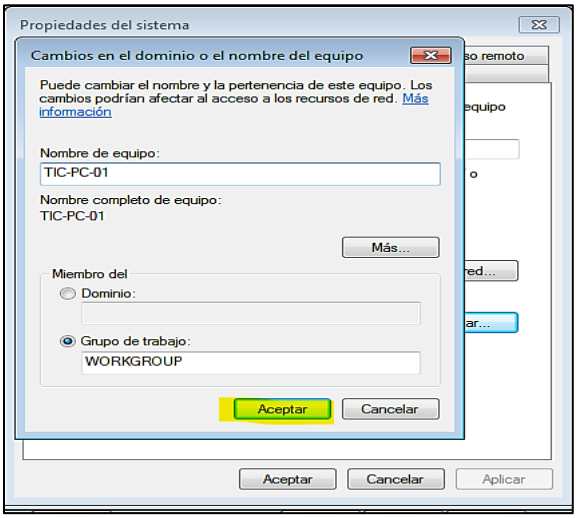
Cambiar nombre del equipo



Posteriormente, se despliega la ventana cambios en el dominio o nombre del equipo como se muestra en la *figura 92*, en la cual se sigue una normativa por departamento luego se da clic en aceptar.

Figura 92

Asignar un nombre al equipo



Luego, se retorna a la ventana propiedades del sistema como se muestra en la *figura 93*, en la cual se da clic en aceptar para que se acepten los cambios.

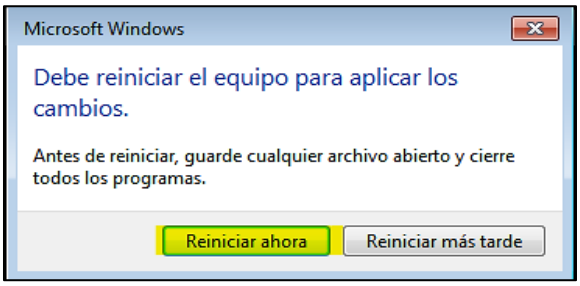
Figura 93

Cerrar la configuración

Finalmente, se despliega la ventana Microsoft Windows como se muestra en la *figura 94*, en la cual se debe dar clic en aceptar para que se acepten los cambios y se pueda reiniciar el equipo ahora.

Figura 94

Reinicio del equipo

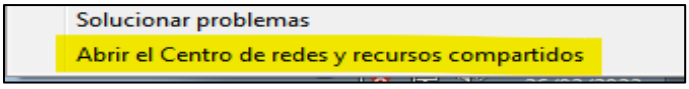


3.3.14. Configuración del DNS del dominio

Para que el equipo pueda unirse al dominio como se muestra en la *figura 89***,** primero se debe configurar la dirección IP de los servidores controladores de dominio en los campos de DNS, por ello dar clic derecho sobre el icono de red de la parte inferior y clic en abrir el centro de redes y recursos compartidos.

Figura 95

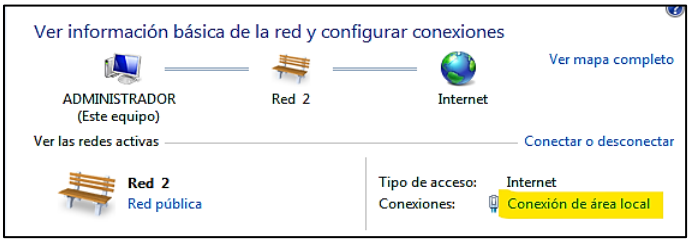
Centro de redes y recursos compartidos.



Luego, se abre la ventana información básica de la red y configurar conexiones como se muestra en la *figura 96*, y dar clic sobre la conexión de área local.

Figura 96

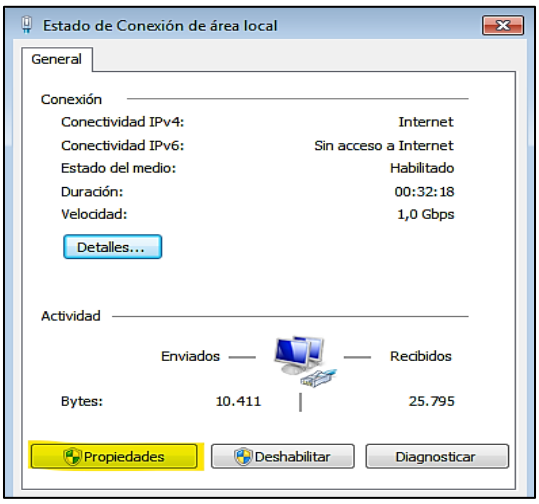
Información básica de la red y configurar conexiones



Posteriormente, se abre la ventana estado de conexión de área local como se muestra en la *figura 97***,** se procede a dar clic en propiedades.

Figura 97

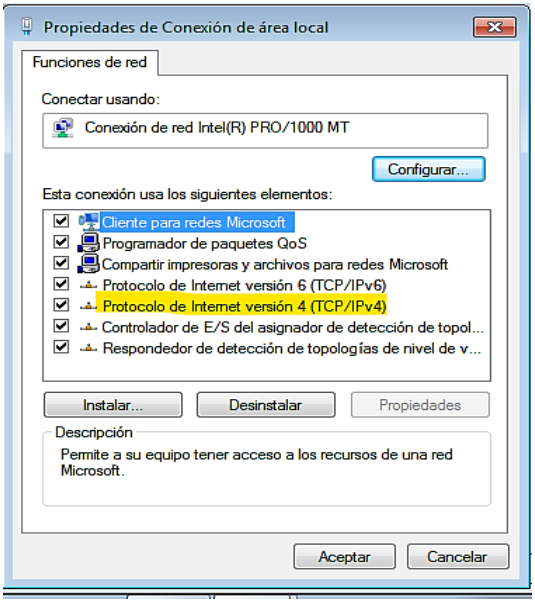
Propiedades de la configuración de red



Luego, se abre la ventana propiedades conexión de área local como se muestra en la *figura 98***,** en la cual se debe seleccionar la opción protocolo de internet versión 4 (TCP/IPv4).

Figura 98

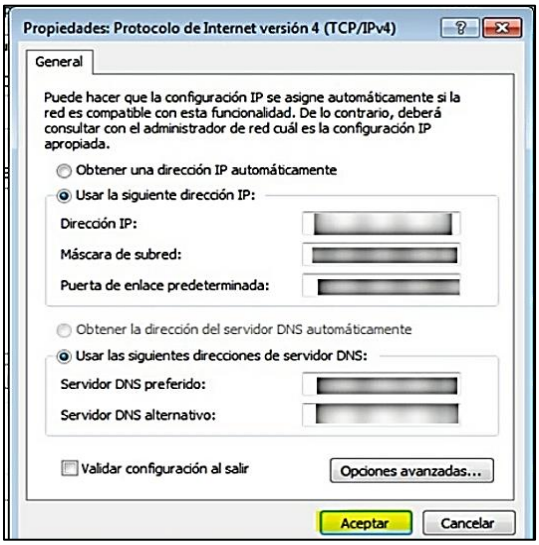
Configuración de IPv4



Posteriormente, se abre la ventana propiedades del protocolo de internet versión 4 (TCP/IPv4) como se muestra en la *figura 99,* el cual aparece las opciones de DNS preferido y alternativo ingresar las direcciones IP de los servidores controladores de dominio y luego dar clic en aceptar.

Figura 99

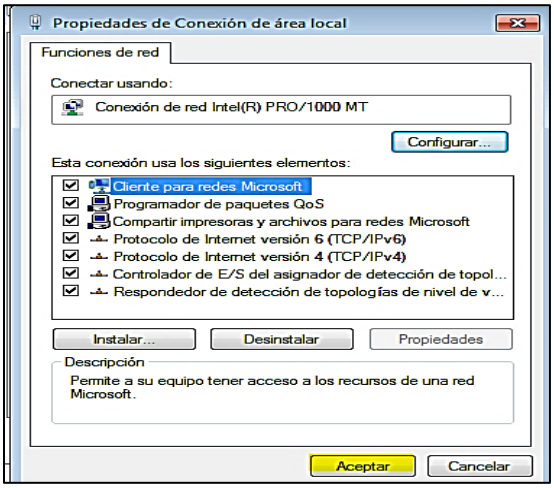
Propiedades del protocolo de internet versión 4 (TCP/IPv4)



Luego, se regresa a la ventana propiedades conexión de área local como se muestra en la *figura 100,* y dar clic en la opción aceptar.

Figura 100

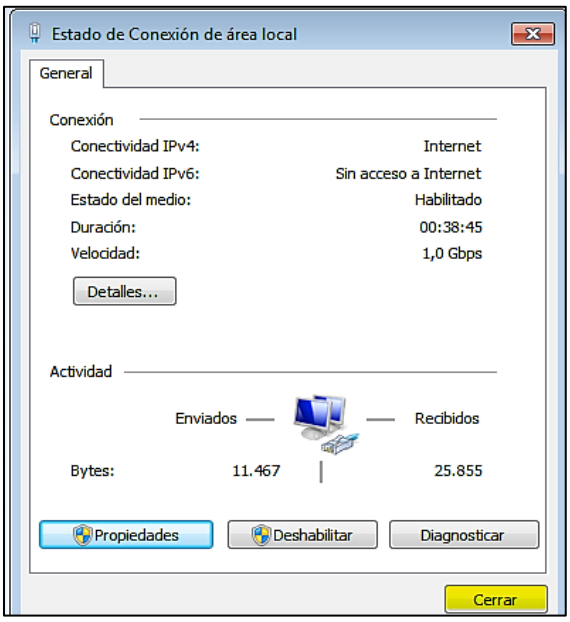
Aceptar propiedades de área local



Posteriormente, se regresa a la ventana estado de conexión de área local como se muestra en la *figura 101***,** y dar clic en la opción aceptar.

Figura 101

Cerrar el estado de conexión de área local

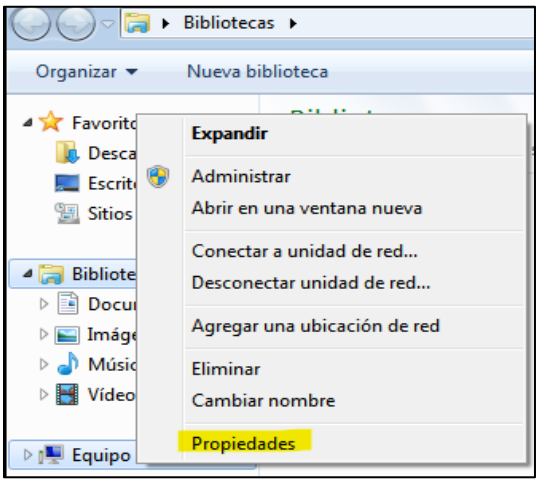


3.3.15. Unir al dominio

Para unir al dominio un equipo como se muestra en la *figura 102***,** primero se debe clic derecho en equipo y luego en propiedades.

Figura 102

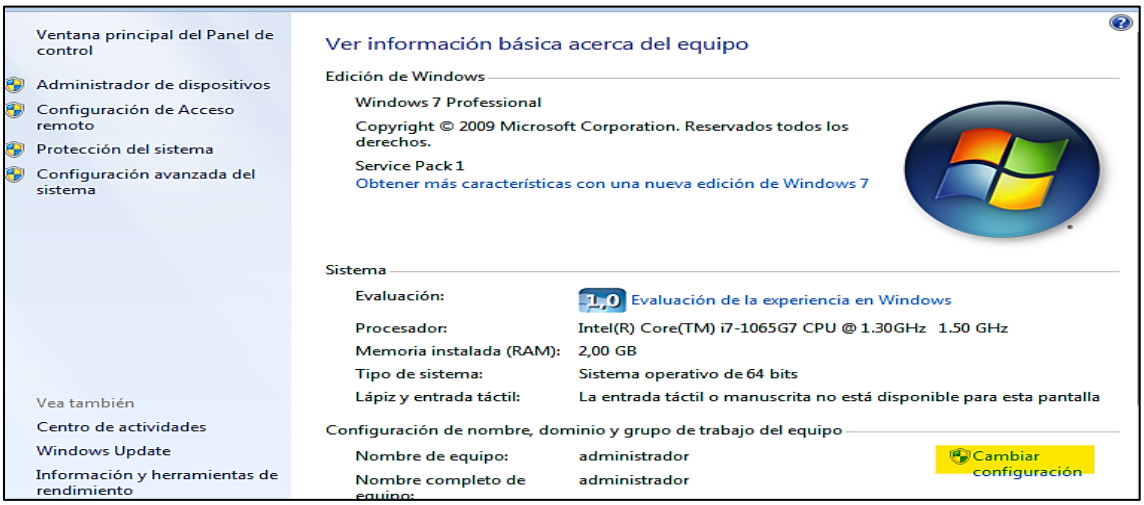
Propiedades del equipo



Posteriormente, en la ventana de información básica del equipo como se muestra en la *figura 103***,** en la inferior derecha se procede a seleccionar la opción cambiar configuración.

Figura 103

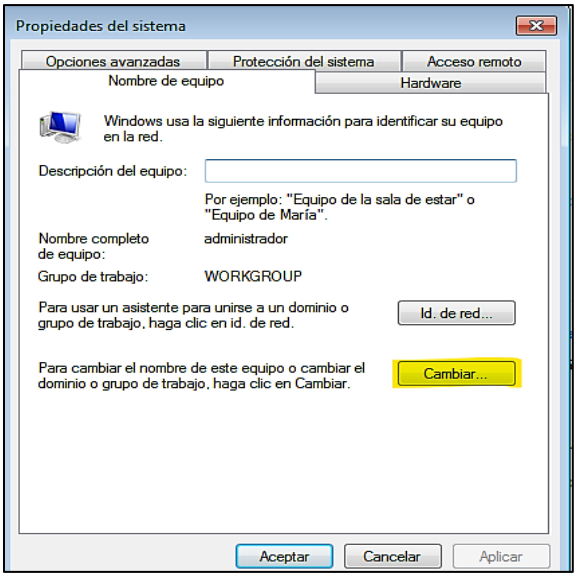
Información básica del equipo



Luego, se despliega la ventana propiedades del sistema como se muestra en la *figura 104*, en la cual se debe dar clic en la opción cambiar.

Figura 104

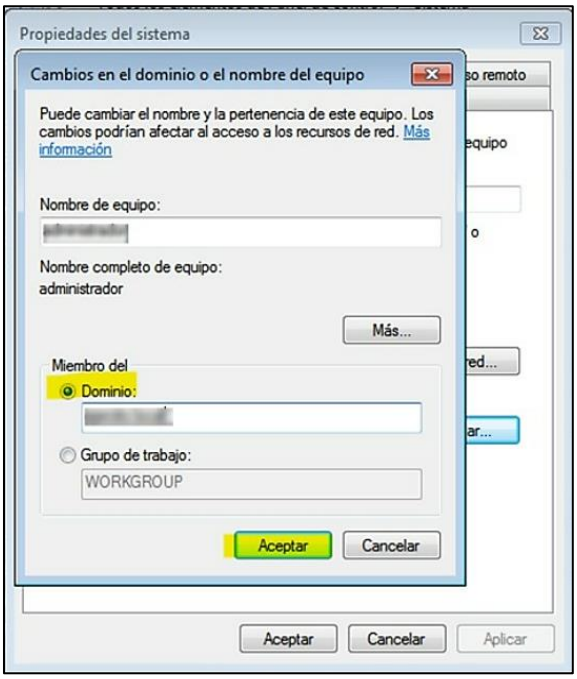
Cambiar propiedades del sistema



Posteriormente, se despliega la ventana cambios en el dominio o nombre del equipo como se muestra en la *figura 105*, en la cual ingresar el dominio de la institución, luego se da clic en aceptar.

Figura 105

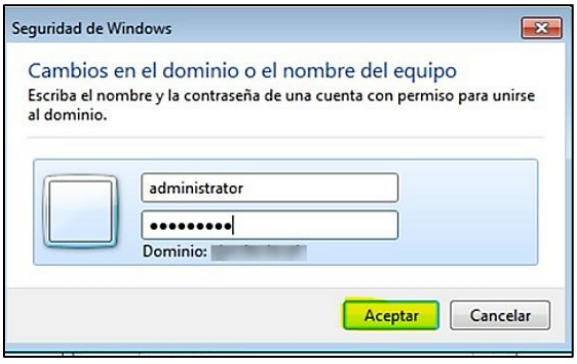
Ingresar nombre del dominio



Luego, se despliega la ventana seguridad de Windows como se muestra en la *figura 106*, en la cual para unirse al dominio ser requiere ingresar el usuario y clave del administrador del dominio para realizar la conexión.

Figura 106

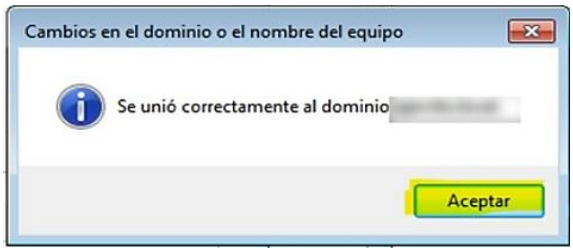
Cambios en el dominio



Posteriormente, se despliega la ventana cambio en el dominio o el nombre del equipo como se muestra en la *figura 107*, que notifica que se ha unido correctamente al dominio y dar clic en aceptar.

Figura 107

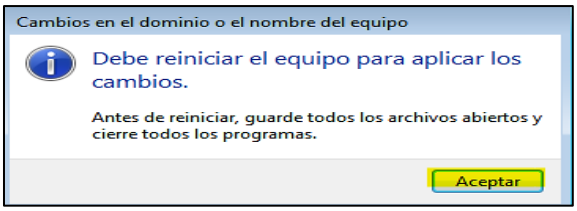
Verificación de conexión al dominio



Luego, se despliega la ventana cambio en el dominio o el nombre del equipo como se muestra en la *figura 108*, en la cual se establece que una vez unido al dominio se debe reiniciar para aplicar los cambios y dar clic en aceptar.

Figura 108

Reinicio del equipo



Posteriormente, una vez reiniciado el equipo como se muestra en la *figura 109*, se debe iniciar sesión con otro usuario ya que el que se tiene es por defecto de la maquina y se requiere del que se creó en el entorno del Active Directory.

Figura 109

Acceso a otro usuario

Luego, en la ventana otro usuario como se muestra en la *figura 110*, se debe ingresar el usuario y clave del dominio asignada por el administrador.

Figura 110

Ingresar usuario y clave del dominio

Posteriormente, en la ventana otro usuario como se muestra en la *figura 111*, pide que se cambie la contraseña del usuario antes de iniciar sesión por primera vez.

Figura 111

Cambio de clave del dominio

Finalmente, en la ventana otro usuario como se muestra en la *figura 112*, una vez cambiado la contraseña permite ingresar automáticamente al entorno de trabajo para el nuevo usuario.

Figura 112

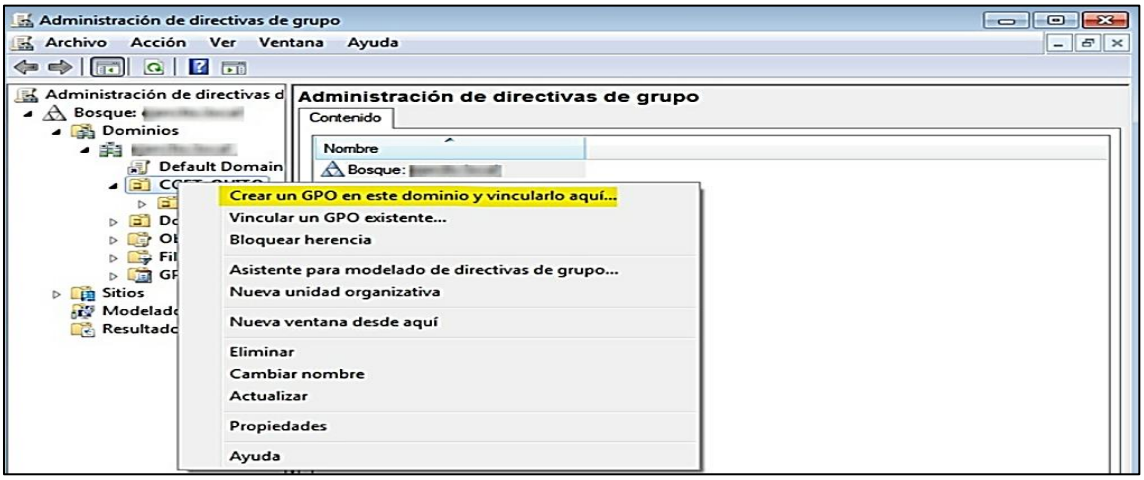
Inicio del proceso

3.3.16. Administración de políticas de usuarios

Inicialmente en la herramienta administración de directivas de grupo como se muestra en la *figura 113***,** se puede ver la estructura organizacional y crear políticas según lo necesidad para cada uno de los departamentos, por ello se debe dar clic derecho en la unidad organizacional a establecer la política y en crear un GOP en este dominio.

Figura 113

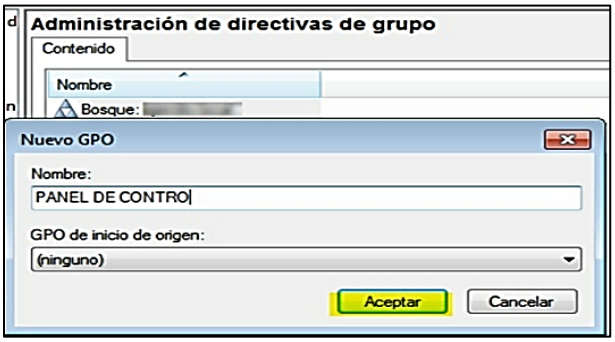
Crear una GOP



Posteriormente, en la ventana administración de directivas de grupo como se muestra en la *figura 114* y se procede a colocar el nombre del GPO que se va aplicar al departamento y se procede a dar clic en aceptar.

Figura 114

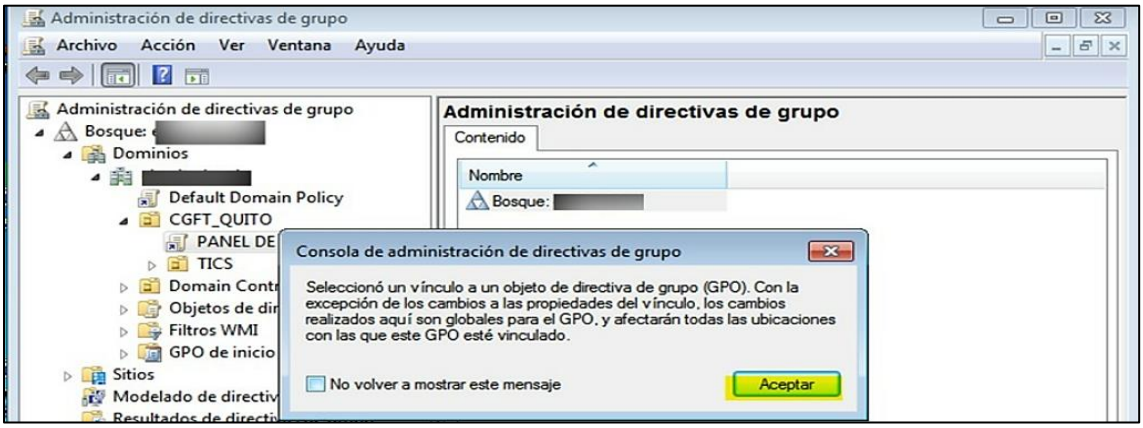
Nombre de la GOP



Luego, en la misma ventana administración de directivas de grupo como se muestra en la *figura 115* y una vez creada la nueva GOP o política se debe dar doble clic en “Panel de control” en donde se despliega la ventana control de administración de directivas de grupo y se procede a dar clic en aceptar.

Figura 115

Aceptación de términos de la GOP



Posteriormente, en la ventana administración de directivas de grupo como se muestra en la *figura 116***,** una vez realizado el paso anterior nuevamente se procede a realizar clic derecho en la GOP “panel de control” y seleccionar editar la política ya que por defecto se crea sin algunos parámetros activados.

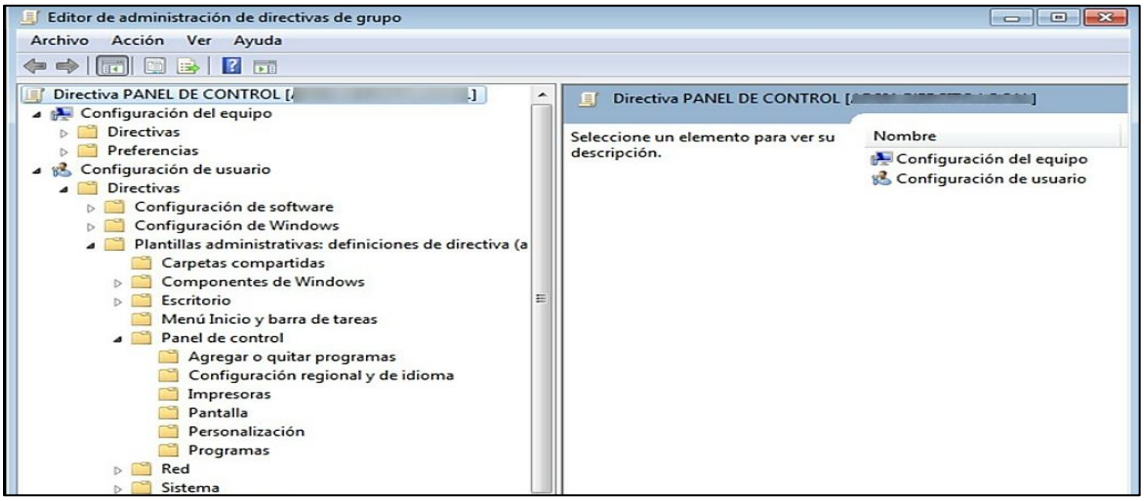
Figura 116

Ventana de configuración para la GOP

Luego, en la ventana editor administración de directivas de grupo como se muestra en la *figura 117*, aquí se identifica todas las políticas a establecer a nivel equipo físico independientemente del usuario, el mismo que se va aplicar al perfil de cada usuario.

Figura 117

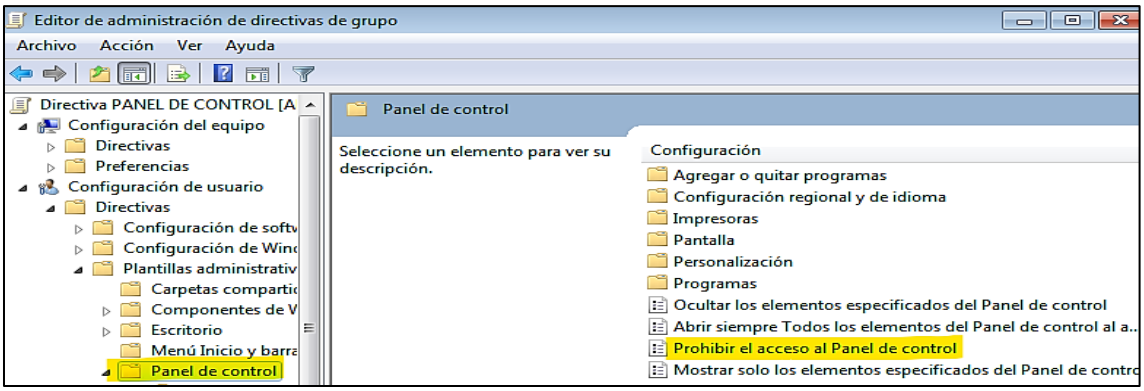
Lista de GOP



Posteriormente, en la ventana editor administración de directivas de grupo como se muestra en la *figura 118*, en la cual para activar todos los parámetros de la GOP "panel de control" se realiza doble clic en la misma y luego se procede a seleccionar prohibir el acceso a panel de control.

Figura 118

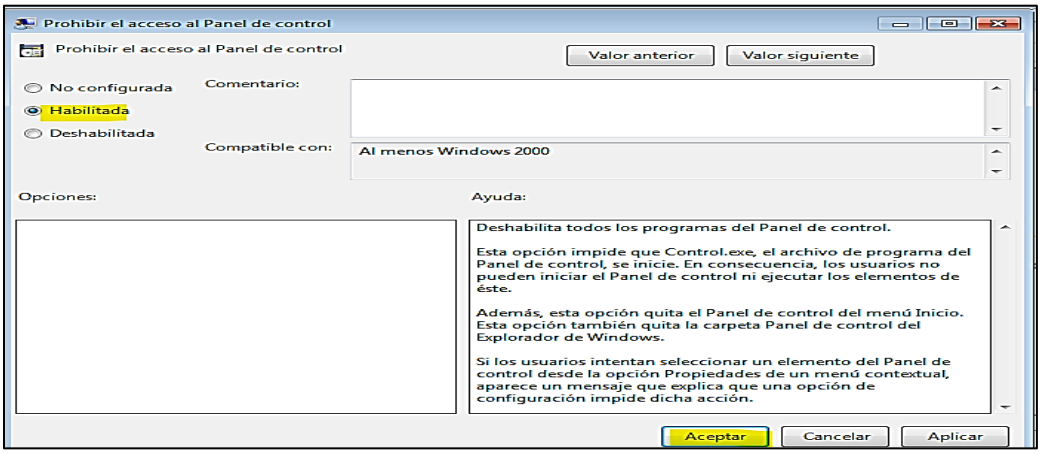
Ventana de accedo a editar la GOP



Finalmente, en la ventana prohibir el acceso al panel de control como se muestra en la *figura 119*, se procede habilitar la GOP terminando la edición de la política este paso se realiza para cualquier tipo de GOP que se quiera agregar con fines de seguridad de administración.

Figura 119

Habilitar GOP

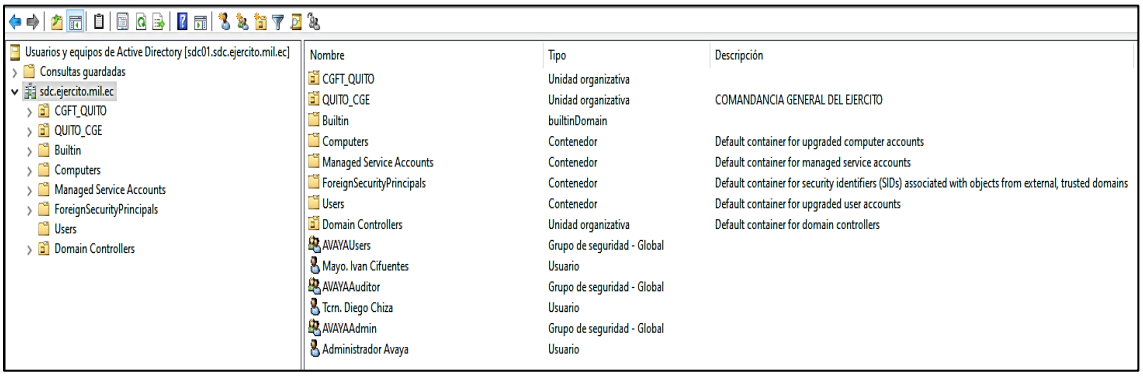


3.3.17. Administración y estructura de la UO

Para iniciar con la administración y estructura como se muestra en la *figura 120,* se crea las 2 principales unidades organizativas, teniendo en cuenta que deben estar asignadas con el nombre del departamento que es el encargado de realizar la administración.

Figura 120

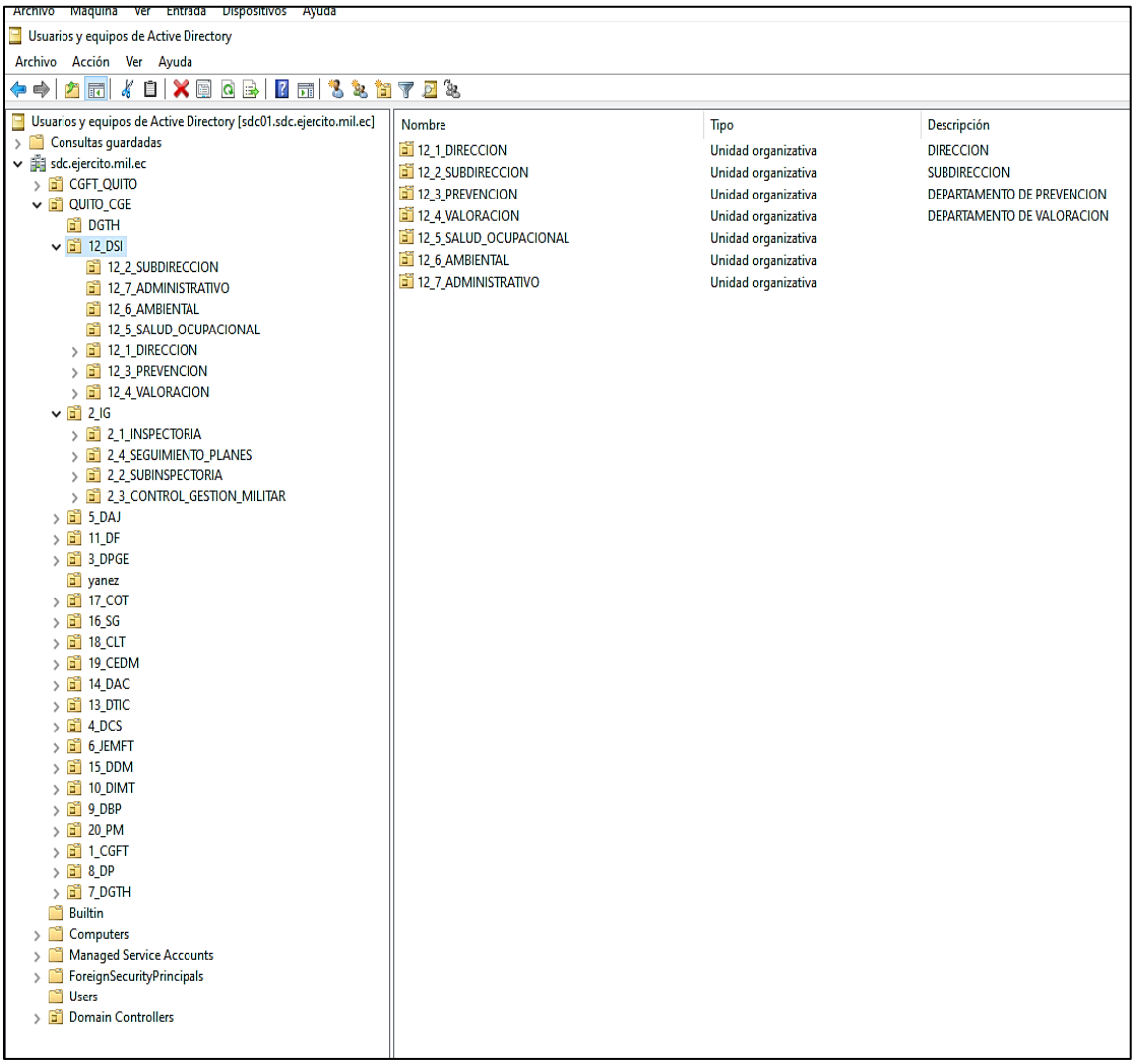
Unidades organizativas



Luego, se despliega las subunidades creadas como se muestra en la *figura 121***,** las mismas que pertenecen a cada uno de los departamentos de la CGFT.

Figura 121

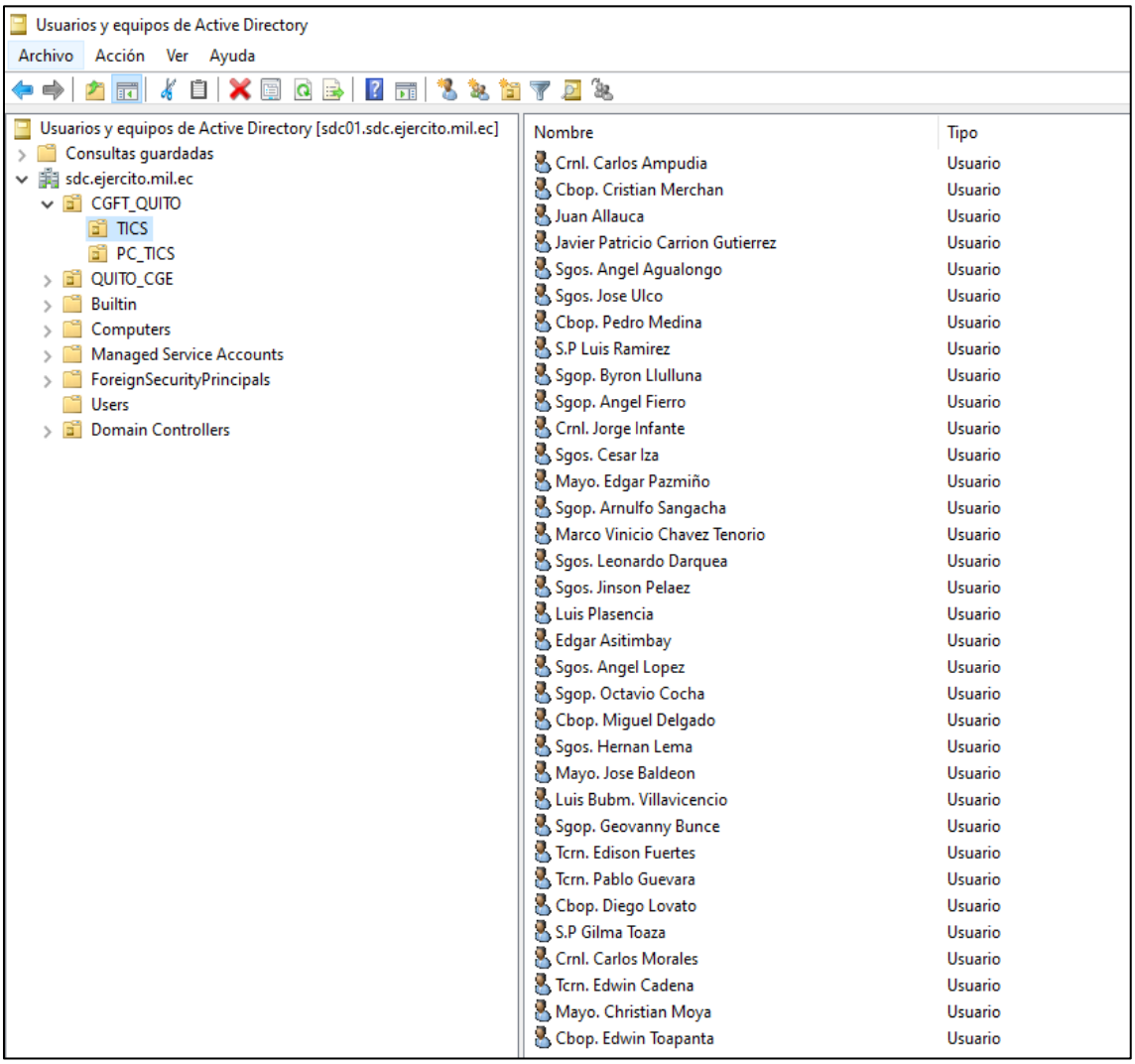
Subunidades organizativas



Finalmente, se despliega las creados en las subunidades organizativas creadas como se muestra en la *figura 121***,** las mismas que serán designadas a cada uno de los equipos en los departamentos.

Figura 122

Vista de usuarios



Capítulo IV

Conclusiones

- Se identifico que dentro de los recursos necesarios para la implementación del controlador de dominio se requirió del software de Ubuntu server 18.04 LTS, cuyo fin fue obtener una mayor seguridad dentro del manejo de la información clasificada de la CGFT, además del servicio de samba cuyo objetivo fue brindar apoyo con respecto a los componentes fundamentales para que el controlador de dominio cumpla con la funcionalidad de un Active Directory, del servicio de administración remota Windows6.1-KB958830 que permitió administrar de una forma adecuada y más rápida la herramienta usuarios y equipos de Active Directory.

- Se realizó la implementación del controlador de dominio mediante la instalación de Ubuntu Server 18.04 LTS, obteniendo así una mayor seguridad informática ya que este es un software libre (Open Sourse), sin embargo se debe tener en cuenta que para la instalación los comandos deben ser ejecutados de manera secuencial y lógica, además se realizó la configuración de la tarjeta de red con una dirección IP estática la misma que permitirá unir al dominio por la dirección DNS, la instalación del servicio SSH para el acceso remoto obteniendo así una instalación más eficiente y rápido y el servicio samba con el protocolo Ldav que permitió brinda los servicios de carpetas compartidas de una red.

- Se realizó la instalación de la herramienta de administración remota Windows 6.1-KB9588 que permitió obtener la interfaz gráfica de la administración de usuarios y equipos de Active Directory y poder crear la estructura de la unidad organizativa UO y manuales de ingresó de equipos al dominio así como se crearon cuentas para cada uno de los usuarios, dependiendo del departamento

y la función de los usuarios se restringió, se habilitado ciertos privilegios, a de cuerdo a la función que desempaña , para ciertos usuario se habilitó privilegios que por la función deben tener habilitados ciertos servició de red y de acceso, además se establecieron políticas de uso de active directory en donde los usuarios no podrán acceder a páginas que no sean de índole militar.

Recomendaciones

- Se recomienda trabajar con software de código abierto Open Sourse permitiendo tener una mayor seguridad al resguardar la información digital de los departamentos, de la misma manera utilizar versiones de software que estén en ejecución y sean recomendadas evitando las versiones actuales que se encuentran en prueba y lograr el rendimiento esperado.

- Se recomienda que para crear el controlador de dominio en el software de código abierto en primera instancia realizar la configuración de la tarjeta de red de una manera correcta respetando los espacios de jerarquía que tiene cada línea de código antes de realizar cualquier instalación de servicios y antes de ingresar los equipos al dominio se debe realizar un respaldo de la información, también es recomendable realizar la actualización de los sistemas operativos a Windows profesionales.

- Se recomienda que para el cumplimiento de las políticas de seguridad es necesario capacitar al personal de las restricciones y ventajas que estas ofrecen en cuanto a la seguridad de información y datos, estas políticas están dirigidas a los grupos y a los usuarios de cada equipo informático, el incumplimiento de estas políticas puede vulnerar la información que el usuario o grupo manejen dentro de cada departamento, o afectar a todo el grupo de trabajo.

Bibliografía

Ayovi, J. (2021). ***Análisis de las malas prácticas en active directory mediante herramientas de pentesting y mitigación de vulnerabilidades a través de un marco metodológico de seguridad.*** Guayaquil: Universidad de Guayaquil. Obtenido de http://repositorio.ug.edu.ec/bitstream/redug /55985/1/AYOVI_ GRUEZO_%20JERSON_PAUL.pdf

Birtlh. (31 de 03 de 2020). ***Acciones sobre el servicio de directorio.*** Obtenido de https://ikastaroak.birt.eus/edu/argitalpen/backupa/20200331/1920k/es/ASIR/ASO /ASO03/es_ASIR_ASO03_Contenidos/website_5_acciones_sobre_el_servicio_d e_directorio.html

Borrero Nuñez, O. (2017). ***Active directory (directorio activo) sistema de seguridad, control y privacidad de la informacion en la gobernacion deltolima.*** Tolima: Gobernación de Tolima. Obtenido de https://core.ac.uk/download/pdf/270126 161.pdf

Dell. (26 de 07 de 2018). ***Desventajas del active directory.*** Obtenido de http://pson linehelp.equallogic.com/es/V6.0/Content/bomre/LDAP/ldap-taskref/ldap_ref _adv_disadv_ad_users_groups.htm

Ediciones-eni. (16 de 09 de 2018). ***Controladores de dominio***. Obtenido de https://www.ediciones-eni.com/open/mediabook.aspx?idR=5a7fe2be6 8cbd7b8e914ec5e588d9bc1

Ejercito Ecuatoriano. (03 de 2020). ***Estructura Organica***. Obtenido de https://ejercitoecuatoriano.mil.ec/institucion/fftt/objetivo-institucional

Ejercito Ecuatoriano. (29 de 03 de 2020). ***Objetivo Institucional*.** Obtenido de https://ejercitoecuatoriano.mil.ec/institucion/fftt/objetivo-institucional

Ejercito Ecuatoriano. (03 de 2020). ***Reseña Historica**.* Obtenido de https://ejercitoecuatoriano.mil.ec/institucion/fftt/resena-historica

Ephesos Software. (04 de 07 de 2019). ***Política de grupo de Windows** ¿Qué es y cómo usarlo?* Obtenido de https://es.ephesossoftware.com/articles/windows/ windows-group-policy-what-is-it-and-how-to-use-it.html

Gomar, J. (16 de 07 de 2019). ***Directorio Activo**.* Obtenido de https://www.tuexperto .com/2019/07/16/active-directory-que-es-y-para-que-sirve/

Google Sites. (18 de 09 de 2011). ***Ventajas y desventajas del manual de usuario.*** Obtenido de https://sites.google.com/site/manualhusuario/porceso/ventajas-y-desventajas

Martinez, P. (21 de 11 de 2008). ***Active Directory en imágenes**, la estructura lógica, árboles, dominios, bosques.* Obtenido de https://blog.soporteti.net/active-directory-la-estructura-logica-arboles-dominios-bosques/

Microsoft. (08 de 11 de 2021). ***Introducción a Active Directory Domain Services.*** Obtenido de https://docs.microsoft.com/es-es/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview

Msinetworks. (16 de 03 de 2020). ***¿Qué son los controladores de dominio?*** Obtenido de https://msinetworks.com.do/en/blog/que-son-los-controladores-de-dominio/

Msinetworks. (16 de 03 de 2020). ***Que son los controladores de dominio***. Obtenido de https://msinetworks.com.do/en/blog/que-son-los-controladores-de-dominio/

Muñoz , J. (2020). ***Estandarización y estudio de tiempos para el mejoramiento del proceso productivo en la industria láctea inladec.*** Ambato: Universidad Tecnica de Ambato.

Openexpoeurope. (15 de 04 de 2021). ***¿Qué es el open source y cómo puede ayudarte?*** Obtenido de https://openexpoeurope.com/es/open-source-puede-ayudarte/

Paessler. (20 de 12 de 2018). ***Active Directory Structure***. Obtenido de https://www.paessler.com/es/it-explained/active-directory

Paessler. (20 de 12 de 2018). ***Otros servicios de Active Directory*****.** Obtenido de https://www.paessler.com/es/it-explained/active-directory

Ranchal , J. (25 de 03 de 2021). ***Cómo mejorar el control de tu PC con las directivas de grupo de Windows***. Obtenido de https://www.muycomputer.com/2021/03/25/directivas-de-grupo-de-windows/

Redhat. (08 de 10 de 2019). ***¿Cuáles son los valores del open source?*** Obtenido de https://www.redhat.com/es/topics/open-source/what-is-open-source

Reparar.info. (16 de 08 de 2021). ***Configuración de una política de contraseña de dominio en Active Directory*****.** Obtenido de https://reparar.info/configuracion-de-una-politica-de-contrasena-de-dominio-en-active-directory/

Robayo Solano, A. (2018). ***Instalación y configuración del Zentyal Server 5.1 servicios como DNS, DHCP, Controladores de dominio, Cortafuegos, Proxy no Transparente y VPN.*** Colombia: Universidad Nacional Abierta y a Distancia UNAD. Obtenido de https://repository.unad.edu.co/handle/10596/18491

Ruiz, P. (15 de 08 de 2013). ***Estructura de directorio activo***. Obtenido de http://somebooks.es/3-2-conceptos-basicos-en-una-estructura-de-directorio-activo/

Scielo. (07 de 2017). ***Manuales de procedimientos*** . Obtenido de http://scielo.sld.cu /scielo.php?script=sci_arttext&pid=S2218-36202017000300038

Servidoresadmin.com. (2022). ***Apt-get update vs apt-get upgrade en linux.*** Obtenido de https://www.servidoresadmin.com/apt-get-update-vs-apt-get-upgrade-en-linux-usos-y-diferencias/#:~:text=Apt%2Dget%20update% 20sirve% 20para ,list%2C%20pero%20no%20instala%20nada.

Simad. (26 de 09 de 2017). ***Active Directory de Microsoft y sus ventajas potenciales.*** Obtenido de https://www.si-mad.com/active-directory-de-microsoft-y-sus-ventajas-potenciales/

Sites.google. (17 de 11 de 2014). ***Descripcion de la Metodologia MSF***. Obtenido de https://sites.google.com/site/aessl13g314/practica-2/2-1

Softgrade. (2021). ***Tipos de manuales***. Obtenido de https://softgrade.mx/manual-de-procedimientos/

Suárez Varela, E. (2019). ***Implementación de un sistema de prevención de perdida de datos, con políticas de seguridad, mediante el control de dominio por medio de una herramienta de terceros***. Villavicencio: Universidad Cooperativa de Colombia. Obtenido de https://repository.ucc.edu.co/bitstream/20.500.12494 /12736/1/2016_implementacion_sistema_prevencion_.pdf

Tecnozero. (26 de 04 de 2019). ***Directorio activo de Microsoft:*** *¿Qué es? ¿Qué ventajas tiene para la empresa?* Obtenido de https://www.tecnozero.com/blog/directorio-activo-de-microsoft-que-es-que-ventajas-tiene-para-la-empresa/

Tecnozero. (26 de 04 de 2019). ***Directorio Activo de Windows,*** *¿qué es?* Obtenido de https://www.tecnozero.com/blog/directorio-activo-de-microsoft-que-es-que-ventajas-tiene-para-la-empresa/

Ubuntu Manpage Repository. (2019). ***Netplan apply*****.** Obtenido de http://manpages.ubuntu.com/manpages/impish/man8/netplan-apply.8.html

Anexos